CURVES $\mathcal{C}$ THAT ARE CYCLIC TWISTS OF $Y^2 = X^3 + c$ AND THE RELATIVE BRAUER GROUPS $Br(k(\mathcal{C})/k)$

Darrell E. Haile, Ilseop Han, Adrian R. Wadsworth

Let k be a field with $char(k) \neq 2, 3$. Let $\mathcal{C}_f$ be the projective curve of a binary cubic form f, and $k(\mathcal{C}_f)$ the function field of $\mathcal{C}_f$. In this paper we explicitly describe the relative Brauer group $Br(k(\mathcal{C}_f)/k)$ of $k(\mathcal{C}_f)$ over k. When f is diagonalizable we show that every algebra in $Br(k(\mathcal{C}_f)/k)$ is a cyclic algebra obtainable using the y-coordinate of a k-rational point on the Jacobian $\mathcal{E}$ of $\mathcal{C}_f$. But when f is not diagonalizable, the algebras in $Br(k(\mathcal{C}_f)/k)$ are presented as cup products of cohomology classes, but not as cyclic algebras. In particular, we provide several specific examples of relative Brauer groups for $k = \mathbb{Q}$, the rationals, and for $k = \mathbb{Q}(\omega)$ where ω is a primitive third root of unity. The approach is to realize $\mathcal{C}_f$ as a cyclic twist of its Jacobian $\mathcal{E}$, an elliptic curve, and then apply a recent theorem of Ciperiani and Krashen.

§1. Introduction

Let k be a field of characteristic not 2 or 3, and let $\mathcal{C}_f$ be the smooth projective curve over k given by the equation $Z^3 = f(X, Y)$, where

$$f(X, Y) \;=\; AX^3 + 3BX^2Y + 3CXY^2 + DY^3 \in k[X, Y] \tag{1.1}$$

is a nongedenerate binary cubic form. Let $k(\mathcal{C}_f)$ be the function field of $\mathcal{C}_f$ over k. The goal of this paper is to compute the relative Brauer group $Br(k(\mathcal{C}_f)/k)$, i.e., the kernel of the scalar extension map $Br(k) \to Br(k(\mathcal{C}_f))$. The curve $\mathcal{C}_f$ has genus 1, and is therefore a principal homogeneous space of the elliptic curve $\mathcal{E}$ which is the Jacobian of $\mathcal{C}_f$. It was known long ago by results of Lichtenbaum in [L$_1$, Lemmas 1, 2, 3], [L$_2$, §2] that since $\mathcal{C}_f$ satisfies period = index, the elements of $Br(k(\mathcal{C}_f)/k)$ are parametrized by $\mathcal{E}(k)$, the group of k-rational points of $\mathcal{E}$. But Lichtenbaum's mapping is difficult to use for explicit calculations. The main tool we apply here is a wonderful recent theorem of Ciperiani and Krashen [CK, Th. 2.6.5], which gives a cup product formula for elements of $Br(k(\mathcal{C})/k)$ when $\mathcal{C}$ is what they call a "cyclic twist" of an elliptic curve $\mathcal{E}$. That is, $\mathcal{C}$ is a principal homogeneous space of $\mathcal{E}$ such that $\mathcal{C}$ lies in the image of $H^1(k, \mathcal{T}) \to H^1(k, \mathcal{E})$ for some Galois stable cyclic subgroup $\mathcal{T}$ of $\mathcal{E}(k_s)$. We prove here that for appropriate choices of $\mathcal{E}$ and $\mathcal{T}$, the principal homogeneous spaces over $\mathcal{E}$ that arise from $H^1(k, \mathcal{T})$ are precisely the curves $\mathcal{C}_f$ as above, and we use their result to describe $Br(k(\mathcal{C}_f)/k)$.

Our interest in these particular curves $\mathcal{C}_f$ comes in part from the theory of generalized Clifford algebras. For every homogeneous form $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ of degree d (say), one can define a k-algebra $A_{f,k}$, the Clifford algebra of f over k, to be the quotient of the free associative algebra $k\{u_1, \ldots, u_n\}$ modulo the ideal generated by the set $\{(a_1u_1 + a_2u_2 + \ldots + a_nu_n)^d - f(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}$. In the case where f is a binary cubic form as in (1.1), it was shown by Haile in [H$_1$, Th.1.1$'$] that $A_{f,k}$ is an Azumaya

We would like to thank D. Krashen for some useful conversations, and in particular for his assistance with the proof of Theorem 6.1.

algebra of rank 9 over its center, and that its center is the coordinate ring of the affine curve $Y^2 = X^3 - 27\Delta_f$ where Δ_f is the discriminant of f (see (6.3) below for a formula for Δ_f). It follows that the k-rational points on this curve give rise to simple images of $A_{f,k}$ with center k. In the same paper Haile also showed that if we let $\mathcal{E}_f$ denote the projective closure of this affine curve, then the resulting function from the group of k-rational points on $\mathcal{E}_f$ to $Br(k)$ (sending the point at infinity to 0) is a group homomorphism, and the image of the homomorphism is the relative Brauer group $Br(k(\mathcal{C}_f)/k)$, where $\mathcal{C}_f$ is the curve given above. This point of view can be used to compute $Br(k(\mathcal{C}_f)/k)$ in many cases, such as when k is perfect and $\Delta, -3 \in k^{*2}$. (See the remarks in the proof of Proposition 4.1.) The algebras in the relative Brauer group are all symbol algebras of degree 3 with one component fixed, and the other depending on points on $\mathcal{E}_f(k)$. However, the machinery of Ciperiani and Krashen has wider applicability. Moreover, it is worthwhile to understand the connection between the two approaches.

Here is a description of the theorem of Ciperiani and Krashen that we will be using below: Let $\mathcal{E}$ be a smooth projective elliptic curve over k, and let $\mathcal{T}$ be a finite cyclic subgroup of the group $\mathcal{E}(k_s)$ of points of $\mathcal{E}$ over the separable closure k_s of k. Suppose $char(k) \nmid |\mathcal{T}|$ and $\mathcal{T}$ is setwise stable under the action of the absolute Galois group $G_k = \mathcal{G}al(k_s/k)$. Let $\mathcal{E}'$ be the elliptic curve isogenous to $\mathcal{E}$ such that $\mathcal{T}$ is the kernel of an isogeny $\lambda\colon \mathcal{E} \to \mathcal{E}'$. Let $\mathcal{T}'$ be the kernel of the dual isogeny $\lambda'\colon \mathcal{E}' \to \mathcal{E}$. Then, $\mathcal{T}'$, like $\mathcal{T}$, is cyclic and Galois stable, with $|\mathcal{T}'| = |\mathcal{T}|$. Let $\mathcal{E}(k)$ denote the group of k-rational points of $\mathcal{E}$, and let $\beta\colon \mathcal{E}(k) \to H^1(k, \mathcal{T}')$ be the connecting homomorphism induced on cohomology by the isogeny λ'. Then, $\mathcal{T} \otimes \mathcal{T}' \cong \mu_n$ (the group of n-th roots of unity in k_s). So, we have a cup product pairing $\cup : H^1(k, \mathcal{T}) \times H^1(k, \mathcal{T}') \to H^2(k, \mu_n) \cong {}_nBr(k)$ (the n-torsion of the Brauer group $Br(k)$). Recall that the Weil-Châtelet group of $\mathcal{E}$ is $H^1(k, \mathcal{E})$ (which denotes, by definition, $H^1(G_k, \mathcal{E}(k_s))$. This group classifies the principal homogeneous spaces of $\mathcal{E}$ (see [Si, pp. 290-291]). Take any $\gamma \in H^1(k, \mathcal{T})$, and let $\mathcal{C}$ be the smooth projective curve of genus 1 over k which is the principal homogeneous space of $\mathcal{E}$ determined by the image of γ under the canonical map $H^1(k, \mathcal{T}) \to H^1(k, \mathcal{E})$. Then [CK, Th. 2.6.5] says that $Br(k(\mathcal{C})/k)$ coincides with the image of the map $\mathcal{E}(k) \to Br(k)$ given by

$$P \mapsto \beta(P) \cup \gamma. \tag{1.2}$$

This theorem will be applied here in the case where the elliptic curve $\mathcal{E}$ is the projective closure of $Y^2 = X^3 + c$ for $c \in k^*$. The point at infinity $\mathcal{O}$ is taken as the identity element for the group operation on $\mathcal{E}$. Then $\mathcal{E}$ has a subgroup $\mathcal{T} = \{(0, \sqrt{c}), (0, -\sqrt{c}), \mathcal{O}\}$, which is clearly closed under the action of G_k. It takes some work to identify the curves to which the theorem applies, and to make explicit the maps used in the theorem. In §2 we prove that when $-3c \in k^{*2}$, the cyclic twists of $\mathcal{E}$ determined by $\mathcal{T}$ are exactly the curves $\mathcal{C}_f$ where f is a diagonal form, i.e., $B = C = 0$ in (1.1) above. In §3 we show that the desired isogenous curve $\mathcal{E}'$ is the projective closure of $Y'^2 = X'^3 + d$, where $d = -27c$, and we determine an isogeny $\lambda\colon \mathcal{E} \to \mathcal{E}'$ with kernel $\mathcal{T}$, and also determine the dual isogeny $\lambda'\colon \mathcal{E}' \to \mathcal{E}$, whose kernel is shown to be $\mathcal{T}' = \{(0, \sqrt{d}), (0, -\sqrt{d}), \mathcal{O}'\}$. In addition, we determine the connecting homomorphism $\mathcal{E}(k) \to H^1(k, \mathcal{T}')$ induced by the isogeny λ'. In §4 we apply the machinery to compute $Br(k(\mathcal{C}_f)/k)$, again in the case where $-3c \in k^{*2}$. In §5 we present explicit calculations for examples with $k = \mathbb{Q}$, the rational numbers, or $k = \mathbb{Q}(\omega)$, where ω is a primitive cube root of unity. In §6 we consider cyclic twists when $-3c$ is not a square (the "nondiagonal case"), and show that they are precisely the curves $\mathcal{C}_f$ as above where the discriminant of f is not a square. We again determine the relative Brauer group as cup products as in (1.2), though this no longer gives a representation of the algebras as cyclic algebras. We give some explicit calculations in the nondiagonal case over $\mathbb{Q}$. Finally, in §7 we turn to generalized Clifford algebras and their rings of quotients; we show aspects of their structure that manifest the specialization results proved earlier.

As indicated in the paragraphs above, we will be working with first cohomology groups of Galois modules of order 3. It is useful to view these modules as twisted versions of more familiar modules, as follows: Let $\mathcal{A}$ be a cyclic group of order 3 which is a discrete G_k-module. For any $b \in k^* \setminus k^{*2}$, we define the twisted G_k-module $\mathcal{A}(b)$ to be the group $\mathcal{A}$, but with new G_k-action, denoted $*$, given by, for $a \in \mathcal{A}$ and $\sigma \in G_k$,

$$\sigma * a \;=\; \begin{cases} \sigma \cdot a, & \text{if } \sigma(\sqrt{b}) = \sqrt{b}; \\ (\sigma \cdot a)^{-1}, & \text{if } \sigma(\sqrt{b}) = -\sqrt{b}. \end{cases} \tag{1.3}$$

If $b \in k^{*2}$ we set $\mathcal{A}(b) = \mathcal{A}$ with unchanged G_k-action. Then, for all $b, b' \in k^*$, we have $\mathcal{A}(b)(b') \cong \mathcal{A}(bb')$ as G_k-modules. For example, take $\mathcal{A} = \mathbb{Z}_3$ (which for us always means $\mathbb{Z}/3\mathbb{Z}$ with trivial G_k-action). Then, $\mathbb{Z}_3(-3) \cong \mu_3$, the group of all cube roots of unity in k_s. Also, for $\mathcal{T} = \{(0, \sqrt{c}), (0, -\sqrt{c}), \mathcal{O}\}$ as above, we have $\mathcal{T} \cong \mathbb{Z}_3(c) \cong \mu_3(-3c)$ as G_k-modules. Such twisted modules and their cohomology groups are discussed in more generality in [HKRT, §5] and [KMRT, pp. 416–418]. The following is the key property we need. It is part of [HKRT, Prop. 21].

Proposition 1.1. *Suppose $b \in k^* \setminus k^{*2}$. Let $L = k(\sqrt{b})$, and let τ be the nonidentity k-automorphism of L. The restriction map res: $H^1(k, \mathcal{A}(b)) \to H^1(L, \mathcal{A})$ is injective, and its image is $\{\delta \in H^1(L, \mathcal{A}) \mid \tau(\delta) = -\delta\}$.*

§2. Twists of $Y^2 = X^3 + c$ determined by $H^1(k, \mathcal{T})$, diagonal case

Let k be a field with $char(k) \neq 2, 3$ and let k_s denote the separable closure of k. Fix $c \in k^*$ and let $\Delta = -c/27$. Let $\mathcal{E}$ be the elliptic curve

$$\mathcal{E}\colon Y^2 \;=\; X^3 + c. \tag{2.1}$$

(More accurately, $\mathcal{E}$ denotes the nonsingular projective elliptic curve $Y^2Z = X^3 + cZ^3$, which consists of the points on the affine curve $Y^2 = X^3 + c$ together with the point $\mathcal{O}$ at infinity. Throughout the paper, the term "elliptic curve" always means a projective elliptic curve, and we routinely specify the curve by giving an affine model, as in (2.1).) We denote by $\mathcal{E}(k)$ the group of k-rational points and by $\oplus$ the group operation on $\mathcal{E}$, which is defined so that $\mathcal{O}$ is the identity element. For any point $P = (r, s) \in \mathcal{E}(k_s)$, its additive inverse $-P$ is $(r, -s)$.

Fix once and for all a choice of square root of c in k_s, denoted $\sqrt{c}$. Then, $(0, \sqrt{c})$ is a point of order 3 on $\mathcal{E}$, as one can check by noting that it is an inflection point of $\mathcal{E}$, or by using the addition formula: for $(r, s) \in \mathcal{E}(k_s)$,

$$(r, s) \oplus (0, \sqrt{c}) \;=\; \begin{cases} \left(\frac{-2\sqrt{c}\,r}{s+\sqrt{c}}, \frac{\sqrt{c}\,(s-3\sqrt{c})}{s+\sqrt{c}}\right) & \text{if } s \neq -\sqrt{c}, \\ \mathcal{O} & \text{if } s = -\sqrt{c}. \end{cases} \tag{2.2}$$

This formula can be verified for $s \neq -\sqrt{c}$ by checking that if we put $(r_1, s_1) = \left(\frac{-2\sqrt{c}\,r}{s+\sqrt{c}}, \frac{\sqrt{c}\,(s-3\sqrt{c})}{s+\sqrt{c}}\right)$, then $(r_1, s_1) \in \mathcal{E}(k_s)$ and the points (r, s), $(0, \sqrt{c})$, and $(r_1, -s_1)$ are collinear.

Since $(0, \sqrt{c})$ has order 3 in $\mathcal{E}$, we have the cyclic subgroup of $\mathcal{E}(k_s)$,

$$\mathcal{T} \;=\; \{\, \mathcal{O}, (0, \sqrt{c}), (0, -\sqrt{c}) \,\}. \tag{2.3}$$

This $\mathcal{T}$ is clearly setwise invariant under the action of the absolute Galois group G_k of k, and $\mathcal{T}$ is stabilized by $G_{k(\sqrt{c})}$. As a G_k-module, $\mathcal{T}$ can be viewed as a twisted version of $\mathbb{Z}_3$ or of the group μ_3 of third roots of unity in k_s (see (1.3) above):

$$\mathcal{T} \cong \mathbb{Z}_3(c) \cong \mu_3(\Delta) \quad \text{where} \;\; \Delta = -c/27. \tag{2.4}$$

Hence, we have maps

$$H^1(k,\mathcal{T}) \xrightarrow{\simeq} H^1(k,\mu_3(\Delta)) \xrightarrow{res} H^1(k(\sqrt{\Delta}),\mu_3) \xrightarrow{\simeq} k(\sqrt{\Delta})^*/k(\sqrt{\Delta})^{*3}. \tag{2.5}$$

Thus, when $\sqrt{\Delta} \in k$, $H^1(k,\mathcal{T}) \cong k^*/k^{*3}$. But, when $\sqrt{\Delta} \notin k$, the restriction map *res* is injective since $[k(\sqrt{\Delta})\colon k]$ is prime to the exponent of $\mathcal{T}$, and Proposition 1.1 yields

$$H^1(k,\mathcal{T}) \cong \{\, z \in k(\sqrt{\Delta})^*/k(\sqrt{\Delta})^{*3} \,\big|\, \tau(z) = z^{-1}\}, \tag{2.6}$$

where τ is the nonidentity k-automorphism of $k(\sqrt{\Delta})$.

The Ciperiani-Krashen results (cf. [CK, §2.6]) apply to projective curves $\mathcal{C}$ which are twists of $\mathcal{E}$ by cohomology classes in the image of the map

$$\Psi\colon H^1(k,\mathcal{T}) \longrightarrow H^1(k,\mathcal{E}) \tag{2.7}$$

induced by the inclusion $\mathcal{T} \hookrightarrow \mathcal{E}(k_s)$. We now determine those curves $\mathcal{C}$ in the diagonal case, where $\sqrt{\Delta} \in k$. (See §6 below for the case $\sqrt{\Delta} \notin k$.) Fix a primitive cube root of unity $\omega \in k_s$, and fix the choice of $\sqrt{\Delta}$ so that $\sqrt{c} = 3(2\omega+1)\sqrt{\Delta}$. Let $P = (0,\sqrt{c}) \in \mathcal{T}$. Since we are assuming $\sqrt{\Delta} \in k^*$, we have a G_k-module isomorphism $\mathcal{T} \xrightarrow{\simeq} \mu_3$ given by $P \mapsto \omega$. Take any $t \in k^* \setminus k^{*3}$, and choose some $\epsilon \in k_s$ with $\epsilon^3 = t$. Let $\gamma_t\colon G_k \longrightarrow \mathcal{T}$ be given by

$$\gamma_t(\rho) = \begin{cases} \mathcal{O} & \text{if } \rho(\epsilon) = \epsilon, \\ P & \text{if } \rho(\epsilon) = \omega\epsilon, \\ -P & \text{if } \rho(\epsilon) = \omega^2\epsilon. \end{cases} \tag{2.8}$$

Thus, $\gamma_t \in Z^1(k,\mathcal{T})$, and its cohomology class $[\gamma_t]$ in $H^1(k,\mathcal{T})$ corresponds to $\bar{t} = tk^{*3}$ under the isomorphism $H^1(k,\mathcal{T}) \cong k^*/k^{*3}$.

Proposition 2.1. *Assume that $\sqrt{\Delta} \in k$. For any $t \in k^* \setminus k^{*3}$, the curve $\mathcal{C}_t$ corresponding to $\Psi[\gamma_t] \in H^1(k,\mathcal{E})$ is*

$$\mathcal{C}_t\colon X^3 - tY^3 = -54\sqrt{\Delta}\, t^2 Z^3.$$

Proof. Assume temporarily that $\mu_3 \subseteq k$ (so $\sqrt{c} \in k$). Let $K = k(\epsilon)$ where $\epsilon^3 = t$. Then K is Galois over k. Let $G = \mathcal{G}al(K/k)$ and let σ be the generator of G with $\sigma(\epsilon) = \omega\epsilon$. The cocycle γ_t defined above is the inflation to the absolute Galois group G_k of a cocycle in $Z^1(G,\mathcal{T})$, which we also denote γ_t. Therefore $\gamma_t(\sigma) = P = (0,\sqrt{c})$. The function field $K(\mathcal{E})$ of $\mathcal{E}$ over K is $K(\mathfrak{r},\mathfrak{s})$ with $\mathfrak{s}^2 = \mathfrak{r}^3 + c$. Let $*$ denote the twisted action of G on $K(\mathcal{E})$ determined by γ_t. Thus (cf. [Si, p. 286]), for $f \in K(\mathcal{E})$ and $\rho \in G$, we have $\rho * f = \rho(f) \circ \tau_{\gamma_t(\rho)}$, where $\rho(f)$ denotes the usual action of ρ on f and $\tau_{\gamma_t(\rho)}\colon \mathcal{E} \to \mathcal{E}$ is translation by $\gamma_t(\rho)$, mapping $(r,s) \mapsto (r,s) \oplus \gamma_t(\rho)$. Since $\gamma_t(\sigma) = P = (0,\sqrt{c})$, $\tau_{\gamma_t(\sigma)}$ is given by formula (2.2) above. Hence, the twisted action of σ on $K(\mathcal{E})$ is given by

$$\sigma * \mathfrak{r} = \frac{-2\sqrt{c}\,\mathfrak{r}}{\mathfrak{s}+\sqrt{c}}, \quad \sigma * \mathfrak{s} = \frac{\sqrt{c}\,(\mathfrak{s}-3\sqrt{c})}{\mathfrak{s}+\sqrt{c}}, \quad \text{and} \quad \sigma * \epsilon = \omega\epsilon.$$

This yields by straightforward calculation (as $9\sqrt{\Delta} = -(2\omega+1)\sqrt{c}$)

$$\sigma * (\mathfrak{s} - 9\sqrt{\Delta}) \;=\; \frac{-2\omega^2\sqrt{c}}{\mathfrak{s}+\sqrt{c}}\,(\mathfrak{s}-9\sqrt{\Delta}) \quad\text{and}\quad \sigma * (\mathfrak{s}+9\sqrt{\Delta}) \;=\; \frac{-2\omega\sqrt{c}}{\mathfrak{s}+\sqrt{c}}\,(\mathfrak{s}+9\sqrt{\Delta}).$$

Hence, if we let $M = \epsilon^2(\mathfrak{s}-9\sqrt{\Delta})/\mathfrak{r}$ and $N = \epsilon(\mathfrak{s}+9\sqrt{\Delta})/\mathfrak{r}$, we find that $\sigma * M = M$ and $\sigma * N = N$, and (as $27\Delta = -c$)

$$M^3 - tN^3 \;=\; \frac{t^2}{\mathfrak{r}^3}\big[(\mathfrak{s}-9\sqrt{\Delta})^3 - (\mathfrak{s}+9\sqrt{\Delta})^3\big] \;=\; \frac{-t^2}{\mathfrak{r}^3}\big[54\sqrt{\Delta}(\mathfrak{s}^2+27\Delta)\big] \;=\; -54\sqrt{\Delta}\,t^2. \tag{2.9}$$

The formulas defining M and N show that $\mathfrak{r},\mathfrak{s} \in K(M,N)$. Hence,

$$[K(\mathfrak{r},\mathfrak{s})\colon k(M,N)] \;=\; [K(M,N)\colon k(M,N)] \;\le\; [K\colon k] \;=\; 3 \;=\; |G|.$$

Therefore, $k(M,N)$ is the full fixed field of $K(\mathfrak{r},\mathfrak{s})$ for the twisted G-action; hence, $k(\mathcal{C}_t) = k(M,N)$. Since the smooth projective curve $\mathcal{C}_t$ is determined up to isomorphism by its function field, we have $\mathcal{C}_t$ is the projective variety $X^3 - tY^3 = -54\sqrt{\Delta}\,t^2Z^3$. This completes the proof for the case where $\mu_3 \subseteq k$.

Now, suppose $\mu_3 \not\subseteq k$ and let $\mathcal{D}_t$ be the projective curve $X^3 - tY^3 = -54\sqrt{\Delta}\,t^2Z^3$ over k. By [An, (3.4), (3.5), (3.8)], $\mathcal{D}_t$ has Jacobian $\mathcal{E}$, so it is the curve determined by some $\theta \in H^1(k,\mathcal{E})$. $\mathcal{D}_t$ clearly has an F-rational point in some field F with $[F\colon k]\,\big|\,3$, so $res_{k\to F}(\theta) = 0$ in $H^1(F,\mathcal{E})$. The composition $cor\circ res\colon H^1(k,\mathcal{E}) \to H^1(F,\mathcal{E}) \to H^1(k,\mathcal{E})$ is multiplication by 3, showing that $3\theta = 0$. This tells us that $\theta \in {}_3H^1(k,\mathcal{E})$, the 3-torsion subgroup of $H^1(k,\mathcal{E})$. Since $[k(\mu_3)\colon k] = 2$, the corestriction-restriction argument shows that the horizontal restriction maps in the following commutative diagram of 3-torsion groups are injective:

$$\begin{array}{ccc} H^1(k,\mathcal{T}) & \xrightarrow{res} & H^1(k(\mu_3),\mathcal{T}) \\ {\scriptstyle\Psi}\big\downarrow & & {\scriptstyle\Psi_{k(\mu_3)}}\big\downarrow \\ {}_3H^1(k,\mathcal{E}) & \xrightarrow{res} & {}_3H^1(k(\mu_3),\mathcal{T}) \end{array}$$

Since the earlier argument showed that $\Psi_{k(\mu_3)}\circ res[\gamma_t] = res(\theta)$, the injectivity implies that $\Psi[\gamma_t] = \theta$, i.e., $\mathcal{C}_t \cong \mathcal{D}_t$ over k. $\square$

Corollary 2.2. *For any $a, b \in k^*$, let $\mathcal{C}$ be the projective curve $\mathcal{C}\colon Z^3 = aX^3 + bY^3$. Then $\mathcal{C}$ is a homogeneous space for the elliptic curve with affine model $\mathcal{E}\colon Y^2 = X^3 + c$ where $c = -\frac{27}{4}a^2b^2$, and $\mathcal{C}$ lies in the image of $\Psi\colon H^1(k,\mathcal{T}) \to H^1(k,\mathcal{E})$. Specifically, $\mathcal{C}$ is $\Psi[\gamma_t]$ for $t = -b/a$ and also for $t = a$ and for $t = b$.*

Proof. We have $\Delta = -c/27 = (ab/2)^2 \in k^{*2}$. Take $\sqrt{\Delta} = ab/2$. Then Proposition 2.1 with $t = -b/a$ shows that $\mathcal{C}_{-b/a}$ is the curve $X^3 - (-b/a)Y^3 = -54(ab/2)(-b/a)^2Z^3$, that is, $aX^3 + bY^3 = (-3bZ)^3$, which is clearly isomorphic to $\mathcal{C}$. (If we made the other choice of $\sqrt{\Delta}$, then $\mathcal{C}_{-b/a}$ is $aX^3 + bY^3 = (3bZ)^3$, which is also isomorphic to $\mathcal{C}$.) Likewise, $\mathcal{C}_a$ can be rewritten as $X^3 = aY^3 + b(-3aZ)^3$ and $\mathcal{C}_b$ as $X^3 = a(-3bZ)^3 + bY^3$, so $\mathcal{C} \cong \mathcal{C}_a$ and $\mathcal{C} \cong \mathcal{C}_b$. $\square$

§3. Dual isogenies and a connecting homomorphism

For the elliptic curve $\mathcal{E}\colon y^2 = x^3 + c$ and its subgroup $\mathcal{T} = \{\, \mathcal{O},\ (0, \pm\sqrt{c})\,\}$ as in §2, there is, up to isomorphism, a unique elliptic curve $\mathcal{E}'$ and isogeny $\lambda\colon \mathcal{E} \to \mathcal{E}'$ with $ker(\lambda) = \mathcal{T}$. That is, we have a short exact sequence

$$0 \longrightarrow \mathcal{T} \longrightarrow \mathcal{E} \xrightarrow{\lambda} \mathcal{E}' \longrightarrow 0. \tag{3.1}$$

There is further an isogeny dual to (3.1) (cf. [Si, Ch. III, §6])

$$0 \longrightarrow \mathcal{T}' \longrightarrow \mathcal{E}' \xrightarrow{\lambda'} \mathcal{E} \longrightarrow 0, \tag{3.2}$$

and we need to determine the associated connecting homomorphism $H^0(k, \mathcal{E}) \to H^1(k, \mathcal{T}')$. First, we obtain explicit descriptions of λ, $\mathcal{E}'$, $\mathcal{T}'$, and λ'.

The paper [V] by Vélu describes how to compute the isogeny with kernel U for any finite subgroup U of an elliptic curve. When U is our group $\mathcal{T}$, his prescription is as follows: For a point P of $\mathcal{E}(k_s)$, write $P = (r(P), s(P))$; then for $P \notin \mathcal{T}$,

$$\lambda(P) \;=\; \Bigg(r(P) + \sum_{Q \in \mathcal{T} \setminus \{\mathcal{O}\}} \big(r(P \oplus Q) - r(Q) \big), \quad s(P) + \sum_{Q \in \mathcal{T} \setminus \{\mathcal{O}\}} \big(s(P \oplus Q) - s(Q) \big) \Bigg). \tag{3.3}$$

If $P \in \mathcal{T}$, then $\lambda(P) = \mathcal{O}'$, the point at infinity, which is the identity element of $\mathcal{E}'$. Since $\mathcal{T} \setminus \{\mathcal{O}\} = \{(0, \sqrt{c}), (0, -\sqrt{c})\}$, for $(r, s) \in \mathcal{E}(k_s)$, we set $(r_1, s_1) = (r, s) \oplus (0, \sqrt{c})$ and $(r_2, s_2) = (r, s) \oplus (0, -\sqrt{c})$. Then, by (2.2) above and its analogue for $(0, -\sqrt{c})$,

$$\lambda(r, s) \;=\; (r + r_1 + r_2,\ s + s_1 + s_2) \;=\; \left(\frac{r^3 + 4c}{r^2},\ \frac{s^3 - 9cs}{r^3} \right) \quad \text{if } (r, s) \notin \mathcal{T}, \tag{3.4}$$

and $\lambda(r, s) = \mathcal{O}'$ if $(r, s) \in \mathcal{T}$. (This formula for the isogeny λ also appears as an exercise in [Ca, p. 65, #5].) By [V, (11)] the elliptic curve $\mathcal{E}'$ has Weierstrass model

$$\mathcal{E}'\colon\ Y^2 \;= X^3 + d \quad \text{where } d = -27c.$$

(One can verify this formula for $\mathcal{E}'$ by checking that all the points $\lambda(r, s)$ lie on this curve.)

The isogeny λ has degree $|\mathcal{T}| = 3$. Therefore the kernel $\mathcal{T}'$ of the dual isogeny λ' is the image under λ of the points of $\mathcal{E}$ of order 3 (cf. [Si, p. 84, Theorem 6.1(a)]). The order 3 points $(\widehat{r}, \widehat{s})$ are obtainable as the inflection points of $\mathcal{E}$, i.e., points where $d^2y/dx^2 = 0$. An easy calculus exercise shows that these are the points with ($\widehat{r} = 0$ and $\widehat{s}^2 = c$) or ($\widehat{r}^3 = -4c$ and $\widehat{s}^2 = -3c$). Hence, by computing $\lambda(\widehat{r}, \widehat{s})$ we find

$$\mathcal{T}' \;=\; \{\, \mathcal{O}',\ (0, \sqrt{d}),\ (0, -\sqrt{d})\,\}. \tag{3.5}$$

(We could alternatively have found the points $(\widehat{r}, \widehat{s})$ by using the triplication formula for $\mathcal{E}$ given in [Si, p. 105, Ex. 3.7(d)].) By repeating the process used to find λ, with d replacing c, we obtain an isogeny $\widetilde{\lambda}\colon \mathcal{E}' \to \mathcal{E}''$ with $ker(\widetilde{\lambda}) = \mathcal{T}'$ where $\mathcal{E}''$ is the elliptic curve $\mathcal{E}''\colon Y^2 = X^3 - 27d = X^3 + 27^2c$. To get back to $\mathcal{E}$, use the isomorphism $\iota\colon \mathcal{E}'' \to \mathcal{E}$ given by $(r, s) \mapsto (r/9,\ s/27)$ and $\mathcal{O}'' \mapsto \mathcal{O}$. Thus, the isogeny $\lambda' = \iota \circ \widetilde{\lambda}\colon \mathcal{E}' \to \mathcal{E}$ with kernel $\mathcal{T}'$ is given by

$$\lambda'(r', s') \;=\; \left(\frac{r'^3 + 4d}{9r'^2},\ \frac{s'^3 - 9ds'}{27r'^3} \right) \quad \text{if } (r', s') \notin \mathcal{T}', \tag{3.6}$$

and $\lambda'(r', s') = \mathcal{O}$ if $(r', s') \in \mathcal{T}'$.

Lemma 3.1. *Let $(r,s) \in \mathcal{E}(k_s)$ with $s \neq -\sqrt{c}$. Choose $t \in k_s^*$ with $t^3 = s + \sqrt{c}$, and set $\widehat{t} = r/t$. Let $r' = 6\sqrt{c}\big/(t - \widehat{t}\,)$ and $s' = 9\sqrt{c}(t+\widehat{t}\,)\big/(t-\widehat{t}\,)$. Then $(r', s') \in \mathcal{E}'(k_s)$ and $\lambda'(r', s') = (r, s)$.*

Proof. Since $s \neq -\sqrt{c}$, it follows that $t \neq 0$, and so $\widehat{t}$ is well-defined. Also, by hypothesis we have $\widehat{t}^{\,3} = r^3/t^3 = s - \sqrt{c} \neq s + \sqrt{c} = t^3$. Therefore, $\widehat{t} \neq t$, assuring that r' and s' are well-defined. (The formulas for r' and s' were found by noting that if $(\widetilde{r}', \widetilde{s}') \in \mathcal{E}'(k_s)$ and $\lambda'(\widetilde{r}', \widetilde{s}') = (\widetilde{r}, \widetilde{s})$, then, from (3.6), $\widetilde{s} + \sqrt{c} = [(\widetilde{s}'^3 - 9d\widetilde{s}')/27\widetilde{r}'^3] + \sqrt{c} = \big[(\widetilde{s}' + 9\sqrt{c})/3\widetilde{r}'\big]^3$, and likewise $\widetilde{s} - \sqrt{c} = \big[(\widetilde{s}' - 9\sqrt{c})/3\widetilde{r}'\big]^3$. These equations can be solved to recover $\widetilde{r}'$ and $\widetilde{s}'$.) Note that as $(t - \widehat{t}\,)^3 = 2\sqrt{c} - 3(t - \widehat{t}\,)r = -\big[3(t+\widehat{t}\,)^2(t-\widehat{t}\,) - 8\sqrt{c}\big]$, we obtain $s'^2 - r'^3 = -27c = d$; so $(r', s') \in \mathcal{E}'(k_s)$. Likewise, straightforward calculations show that $(r'^3 + 4d)/9r'^2 = r$ and $s'(s'^2 - 9d)\big/27r'^3 = s$; so, $\lambda'(r', s') = (r, s)$. $\square$

Since $\sqrt{d} = 3\sqrt{-3}\sqrt{c}$, it follows that $\mathcal{T}'$ is a twisted G_k-module, and

$$\mathcal{T}' \;\cong\; \mu_3(c). \tag{3.7}$$

Hence, we have maps

$$H^1(k, \mathcal{T}') \xrightarrow{\simeq} H^1(k, \mu_3(c)) \xrightarrow{res} H^1(k(\sqrt{c}), \mu_3) \xrightarrow{\simeq} k(\sqrt{c})^*/k(\sqrt{c})^{*3}. \tag{3.8}$$

Define the homomorphism

$$\alpha\colon \mathcal{E}(k) \to k(\sqrt{c})^*/k(\sqrt{c})^{*3}, \tag{3.9}$$

to be the composition of maps

$$\mathcal{E}(k) \xrightarrow{\partial} H^1(k, \mathcal{T}') \longrightarrow k(\sqrt{c})^*/k(\sqrt{c})^{*3}, \tag{3.10}$$

where ∂ is the connecting homomorphism $\mathcal{E}(k) = H^0(k, \mathcal{E}) \to H^1(k, \mathcal{T}')$ arising from the short exact sequence (3.2), and the second map is the monomorphism which is the composition of maps in (3.8).

Proposition 3.2. *For $(r,s) \in \mathcal{E}(k)$ with $s \neq -\sqrt{c}$, one has*

$$\alpha(r,s) \;=\; \overline{s + \sqrt{c}} \;\in\; k(\sqrt{c})^*/k(\sqrt{c})^{*3}.$$

Also, if $\sqrt{c} \in k$, then $\alpha(0, -\sqrt{c}) = \overline{4c}$.

Proof. To be consistent with choices of square roots of c and d and cube roots of unity, let ω be a fixed cube root of unity, and let $\eta = 2\omega + 1$, which is a fixed square root of -3. Then set $\sqrt{d} = 3\eta\sqrt{c}$. We use the G_k-module isomorphism $\mathcal{T}' \to \mu_3(c)$ given by $(0, \sqrt{d}) \mapsto \omega$. Since connecting homomorphisms are compatible with restriction maps and the map $res\colon H^1(k, \mathcal{T}') \to H^1(k(\sqrt{c}), \mathcal{T}')$ is injective, it suffices to prove the proposition when $\sqrt{c} \in k$. Assume this. For any $u \in k^*$ and any fixed $\sqrt[3]{u} \in k_s^*$, we have a cocycle $\gamma_u \in Z^1(k, \mathcal{T}')$ given by, for $\sigma \in G_k$,

$$\gamma_u(\sigma) \;=\; \begin{cases} \mathcal{O}' & \text{if } \sigma(\sqrt[3]{u}) = \sqrt[3]{u}, \\ (0, \sqrt{d}) & \text{if } \sigma(\sqrt[3]{u}) = \omega\,\sqrt[3]{u}, \\ (0, -\sqrt{d}) & \text{if } \sigma(\sqrt[3]{u}) = \omega^2\,\sqrt[3]{u}. \end{cases}$$

Our isomorphism $H^1(k,\mathcal{T}') \to k^*/k^{*3}$ of (3.7) is given by $[\gamma_u] \mapsto \overline{u}$. Thus, it suffices to prove that the connecting homomorphism $\partial\colon \mathcal{E}(k) \to H^1(k,\mathcal{T}')$ maps $(r,s) \mapsto [\gamma_{s+\sqrt{c}}]$ when $s \neq -\sqrt{c}$, and $\partial(0,-\sqrt{c}) = [\gamma_{4c}]$.

For $(r,s) \in \mathcal{E}(k)$ with $s \neq -\sqrt{c}$, choose $t \in k_s^*$ with $t^3 = s+\sqrt{c}$, and let $\widehat{t} = r/t$, $\rho = t+\widehat{t}$, and $\delta = t-\widehat{t} \neq 0$. Set $(r',s') = (6\sqrt{c}/\delta,\, 9\sqrt{c}\rho/\delta)$. By Lemma 3.1, $(r',s') \in \mathcal{E}'(k_s)$ and $\lambda'(r',s') = (r,s)$. Then $\partial(r,s)$ is the cohomology class of the cocycle $\zeta\colon G_k \to \mathcal{T}'$ given by $\sigma \mapsto \sigma(r',s') \ominus (r',s')$, where $\ominus$ denotes subtraction in $\mathcal{E}'$. Take any $\sigma \in G_k$. If $\sigma(t) = t$, then also $\sigma(\widehat{t}) = \widehat{t}$, as $\widehat{t} = r/t$ and $x \in k$, so $\sigma(r',s') = (r',s')$. Hence, $\zeta(\sigma) = \mathcal{O}' = \gamma_{s+\sqrt{c}}(\sigma)$. Suppose next that $\sigma(t) = \omega t = \frac{1}{2}(-1+\eta)t$. Then, as $t\,\widehat{t} = r$, we have $\sigma(\widehat{t}) = \omega^{-1}\widehat{t} = \frac{1}{2}(-1-\eta)\widehat{t}$, so that $\sigma(\rho) = \frac{1}{2}(-\rho+\eta\delta)$ and $\sigma(\delta) = \frac{1}{2}(-\delta+\eta\rho)$, which is nonzero as $\delta \neq 0$. Hence,

$$\sigma(r',s') \;=\; \sigma\big(6\sqrt{c}/\delta,\ 9\sqrt{c}\rho/\delta\big) \;=\; \big(12\sqrt{c}/(-\delta+\eta\rho),\ 9\sqrt{c}(-\rho+\eta\delta)/(-\delta+\eta\rho)\big). \tag{3.11}$$

Note that $s'+\sqrt{d} = 3\eta\sqrt{c}(-\eta\rho+\delta)/\delta \neq 0$.

The analogue to formula (2.2) (replacing c by d) combined with (3.11) yields

$$\begin{aligned}
(r',s') \oplus (0,\sqrt{d}) \;&=\; \big(\tfrac{-2\sqrt{d}r'}{s'+\sqrt{d}},\, \tfrac{\sqrt{d}(s'-3\sqrt{d})}{s'+\sqrt{d}}\big)\\
&=\; \big(\tfrac{-36\eta c}{9\sqrt{c}\rho+3\eta\sqrt{c}\delta},\, \tfrac{3\eta\sqrt{c}(9\sqrt{c}\rho-9\eta\sqrt{c}\delta)}{9\sqrt{c}\rho+3\eta\sqrt{c}\delta}\big)\\
&=\; \big(\tfrac{12\sqrt{c}}{\eta\rho-\delta},\, \tfrac{9\sqrt{c}(\rho-\eta\delta)}{-\eta\rho+\delta}\big)\\
&=\; \sigma(r',s').
\end{aligned}$$

Thus, we have $\sigma(r',s') \ominus (r',s') = (0,\sqrt{d})$ when $\sigma(t) = \omega t$. Likewise, if $\sigma(t) = \omega^2 t$, then the analogous calculation (with $-\sqrt{d}$ and $-s$ replacing $\sqrt{d}$ and s) shows that $\sigma(r',s') \ominus (r',s') = (0,-\sqrt{d})$. So our cocycle $\zeta = \gamma_{t^3} = \gamma_{y+\sqrt{c}}$, showing that $\partial(r,s) = [\gamma_{s+\sqrt{c}}]$ whenever $s \neq -\sqrt{c}$. Since ∂ is a homomorphism with $\partial(0,\sqrt{c}) = [\gamma_{2\sqrt{c}}]$ and $(0,-\sqrt{c}) = (0,\sqrt{c}) \oplus (0,\sqrt{c})$, we have $\partial(0,-\sqrt{c}) = [\gamma_{(2\sqrt{c})^2}] = [\gamma_{4c}]$. $\square$

§4. Relative Brauer Groups $Br(k(\mathcal{C})/k)$ for $\mathcal{C}\colon Z^3 = aX^3 + bY^3$

For any $a,b \in k^*$, let $\mathcal{C}$ be the smooth projective genus 1 curve over k,

$$\mathcal{C}\colon\ Z^3 \;=\; a\,X^3 \;+\; b\,Y^3\,, \tag{4.1}$$

and let $k(\mathcal{C})$ be the function field of $\mathcal{C}$ over k. We can now describe the relative Brauer group $Br(K(\mathcal{C})/k)$, as the target of a homomorphism from the k-rational points of the Jacobian of $\mathcal{C}$, which is the elliptic curve $\mathcal{E}$ with Weierstrass model

$$\mathcal{E}\colon\ Y^3 \;=\; X^3 \;+\; c\,, \quad \text{where}\ \ c \;=\; -\tfrac{27}{4}a^2b^2\,. \tag{4.2}$$

The algebras in $Br(k(\mathcal{C})/k)$ are symbol algebras when $\mu_3 \subseteq k$, and are cyclic algebras otherwise. Throughout this section, let ω denote a fixed primitive cube root of unity in k_s^*. If $\omega \in k^*$, let $(t,u;k)_\omega$, or simply $(t,u)_\omega$, denote the 9-dimensional symbol algebra over k with generators i, j and relations $i^3 = t$, $j^3 = u$, and $ij = \omega ji$.

Proposition 4.1. *Let k be a field with $\mu_3 \subseteq k$, and let $a, b \in k^*$. For the projective curve $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ over k with Jacobian $\mathcal{E}$ as in* (4.2)*, there is a surjective group homomorphism*

$$\varphi\colon \mathcal{E}(k) \to Br(k(\mathcal{C})/k) \ \text{ given by } \ (r,s) \mapsto [(a, s+\sqrt{c}\,)_\omega]\,. \tag{4.3}$$

In other words,

$$Br(k(\mathcal{C})/k) \,=\, \{\,[(a, s+\sqrt{c}\,)_\omega] \mid \overline{s+\sqrt{c}} \in im(\alpha) \subseteq k^*/k^{*3}\,\},$$

where α is the map in (3.9) *and Proposition* 3.2.

Proof. (When k is perfect, this was proved in [H_1, Cor. 1.2] and [H_2, Th. 1.2 and Cor. 2.2] using the generalized Clifford algebra of the binary cubic form aX^3+bY^3. The case when k is not perfect is deducible from the perfect case by working back from the perfect hull of k. We give an alternative approach here based on the theorem of Ciperiani and Krashen, since this approach is more readily applicable in other cases. See Proposition 4.4 and §6 below.)

Note that $\sqrt{c} \in k$, as $\omega \in k$. Let $\mathcal{T}$ be the cyclic subgroup $\{\mathcal{O}, (0, \pm\sqrt{c})\}$ of $\mathcal{E}(k)$. By Corollary 2.2 above, $\mathcal{C}$ is the homogeneous space of $\mathcal{E}$ corresponding to $\Psi[\gamma_a]$ in $H^1(k,\mathcal{E})$, where $\gamma_a \in Z^1(k,\mathcal{T})$ is as in (2.8). We have the isogeny (3.1) with kernel $\mathcal{T}$, and its dual isogeny (3.2), with kernel $\mathcal{T}' = \{\mathcal{O}', (\pm\sqrt{d})\}$, where $d = -27c$. Let $\partial\colon \mathcal{E}(k) \to H^1(k,\mathcal{T}')$ be the connecting homomorphism arising from the dual isogeny. By [CK, Th. 2.6.5], $Br(k(\mathcal{C})/k)$ coincides with the image of the map

$$\beta\colon \mathcal{E}(k) \to Br(k) \quad \text{ given by } \quad \beta(r,s) \,=\, \partial(r,s) \cup [\gamma_a]\,, \tag{4.4}$$

where the cup product $\cup$ maps $H^1(k,\mathcal{T}') \times H^1(k,\mathcal{T}) \to H^2(k, \mathcal{T}' \otimes \mathcal{T}) \cong H^2(k,\mu_3) \cong {}_3Br(k)$. Now, $\mathcal{T}' \cong \mathbb{Z}_3(c) \cong \mu_3$ as G_k-modules, since $\sqrt{c} \in k$ and $\mu_3 \subseteq k$. Hence, $H^1(k,\mathcal{T}') \cong k^*/k^{*3}$ and, as shown in Proposition 3.2, under this isomorphism the map ∂ corresponds to $\alpha\colon \mathcal{E}(k) \to k^*/k^{*3}$ given by $(r,s) \mapsto \overline{s+\sqrt{c}}$. Also, $\mathcal{T} \cong \mathbb{Z}_3(d) \cong \mu_3$, and in the isomorphism $H^1(k,\mathcal{T}) \cong k^*/k^{*3}$, $[\gamma_a]$ corresponds to $\overline{a}$. The cup product $H^1(k,\mu_3) \cup H^1(k,\mu_3) \to {}_3Br(k)$ gives rise to the map

$$\kappa\colon k^*/k^{*3} \times k^*/k^{*3} \to {}_3Br(k)$$

given by $(\overline{t}, \overline{u}) \mapsto (u,t)_\omega$. (For, by [Se, p. 207, Prop. 5], the cup product maps the pair $(\overline{t}, \overline{u})$ to the Brauer class of the cyclic algebra $(k(\sqrt[3]{t})/k, \sigma, u)$, where $\sigma(\sqrt[3]{t}) = \omega\sqrt[3]{t}$. This algebra is generated by i and j, where $j^3 = t$, $i^3 = u$ and $iji^{-1} = \omega j$, so $ij = \omega ji$.) Thus, for any $(r,s) \in \mathcal{E}(k)$, we have $\beta(r,s) = \kappa(\overline{s+\sqrt{c}}\,, \overline{a}) = (a, s+\sqrt{c})_\omega$. $\square$

Remark 4.2. (i) If the symbol algebra $(a,b)_\omega$ is nonsplit, then Proposition 4.1 shows that $Br(k(\mathcal{C})/k)$ is nontrivial since $[(a,b)_\omega] \in Br(k(\mathcal{C})/k)$. In fact, since $\omega \in k$, we have $\sqrt{c} \in k$, so the point $(0, \sqrt{c}) \in \mathcal{E}(k)$. This implies that $[(a, 2\sqrt{c})_\omega] \in Br(k(\mathcal{C})/k)$. But, we have

$$(a, 2\sqrt{c})_\omega \,=\, \big(a, 2\sqrt{-\tfrac{27}{4}a^2b^2}\big)_\omega \,\cong\, \big(a, \sqrt{-3}^{\,3}ab\big)_\omega \,\sim\, (a,a)_\omega \otimes (a,b)_\omega \,\sim\, (a,b)_\omega.$$

Note here that -1 is a cube in k, so $(a,a)_\omega \cong (a,-1)_\omega$ is split. We point out also that the converse of this remark is not necessarily true in general. Corollary 4.6 (i) below can be used to provide counterexamples.

(ii) In Proposition 4.1, we can replace a in the symbol algebras by b or by $-b/a$ if this is more convenient for computation. This follows from Corollary 2.2, since the curve $\mathcal{C}$ is represented by $\Psi[\gamma_b]$ and $\Psi[\gamma_{-b/a}]$ as well as by $\Psi[\gamma_a]$.

Now, we consider the case that $\mu_3 \not\subseteq k$. In order to determine $Br(k(\mathcal{C})/k)$ for any field k, we need

Lemma 4.3. *Let k be a field with $\mu_3 \not\subseteq k$, let $L = k(\omega)$, and let $\sigma \in \mathcal{G}al(L/k)$ with $\sigma \neq id$. If $T = L(\sqrt[3]{\xi})$ for $\xi \in L^* \setminus L^{*3}$, then:*

(i) *There is a subfield S of L such that S/k is a cyclic extension of degree 3 if and only if $\sigma(\overline{\xi}) = \overline{\xi}^{\,-1}$ in L^*/L^{*3}.*

(ii) *If $\sigma(\xi) = \xi^{-1}r^3$ for some $r \in k^*$, then $S = k(u)$, where u has minimal polynomial $X^3 - 3rX - (\xi + \sigma(\xi))$ over k.*

Proof. (i) This result is known, see Albert ([A, Th. 2]). In cohomological terms, since $\mu_3 \not\subseteq k$, we have $\mathbb{Z}_3 \cong \mu_3(-3)$ as G_k-modules. Hence, there are maps

$$H^1(k, \mathbb{Z}_3) \xrightarrow{\simeq} H^1(k, \mu_3(-3)) \hookrightarrow H^1(L, \mu_3).$$

This yields an injection $H^1(k, \mathbb{Z}_3) \to L^*/L^{*3}$, whose image is $\{\, \overline{\xi} \in L^*/L^{*3} \mid \sigma(\overline{\xi}) = \overline{\xi}^{\,-1}\}$ by Proposition 1.1 . The cyclic subgroups of $H^1(k, \mathbb{Z}_3)$ classify the cyclic field extensions of k of degree 3, and in field terms, the preceding map takes a cyclic field extension S of k to $\overline{\xi}$ where $S \cdot L = L(\sqrt[3]{\xi})$.

(ii) Let $\epsilon \in T$ with $\epsilon^3 = \xi$. The map σ extends to an automorphism $\widetilde{\sigma}$ of T of order 2 given by $\widetilde{\sigma}(\epsilon) = r\epsilon^{-1}$, and the fixed field of $\widetilde{\sigma}$ is S. Let $u = \epsilon + \widetilde{\sigma}(\epsilon) = \epsilon + r\epsilon^{-1} \in S$. Then, $u \notin k$ since ϵ satisfies a polynomial of degree 2 over $k(u)$ but $[L(\epsilon) : L] = 3$. So, $S = k(u)$. By computing u^3, we see that u is a root of $X^3 - 3rX - (\xi + \sigma(\xi)) \in k[X]$. Since $[k(u) : k] = 3$, this polynomial must be the minimal polynomial of u over k. Let $u' = \omega\epsilon + \widetilde{\sigma}(\omega\epsilon) = \omega\epsilon + \omega^{-1}r\epsilon^{-1}$. Then u' is another root of $min(u, k)$ in S. So, there is a nontrivial k-automorphism of S sending u to u'. This shows directly that S is cyclic Galois over k. $\square$

Lemma 4.3 enables us to give the analogue to Proposition 4.1 when $\mu_3 \not\subseteq k$. In that case we let $L = k(\omega) = k(\sqrt{c})$, and work down from 3-Kummer field extensions of L to cyclic extensions of k.

Proposition 4.4. *Let k be a field with $\mu_3 \not\subseteq k$. For $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ and c, $\mathcal{E}$ as in (4.2), there is a surjective group homomorphism*

$$\varphi\colon \mathcal{E}(k) \to Br(k(\mathcal{C})/k) \ \text{ given by } \ (r, s) \mapsto [(S/k, \tau, a)]$$

where S is the cyclic field extension of k lying in $k\big(\omega, \sqrt[3]{s + \sqrt{c}}\big)$ described in Lemma 4.3.

Proof. The result of [CK] still applies, just as for Proposition 4.1, and it shows that $Br(k(\mathcal{C})/k) = im(\beta)$ for β the map of (4.4). But now, as $\mu_3 \not\subseteq k$, we have $\sqrt{c} \notin k$. Let $L = k(\sqrt{c}) = k(\omega)$, and let σ be the nonidentity k-automorphism of L. We have $\mathcal{T}' \cong \mathbb{Z}_3 \cong \mu_3(c)$ as G_k-modules, and $\mathcal{T} \cong \mu_3$. So the cup product in (4.4) corresponds to the cup product $H^1(k, \mathbb{Z}_3) \times H^1(k, \mu_3) \to {}_3Br(k)$. Here $[\gamma_a] \in H^1(k, \mathcal{T})$ corresponds to $\overline{a} \in k^*/k^{*3} \cong H^1(k, \mu_3)$.

Now, $H^1(k, \mathbb{Z}_3) \cong Hom(G_k, \mathbb{Z}_3)$, which classifies cyclic degree 3 field extensions of k with a specified generator of the Galois group. The restriction map sends $H^1(k, \mathbb{Z}_3) \cong H^1(k, \mu_3(c))$ injectively into $H^1(L, \mu_3) \cong L^*/L^{*3}$. By Proposition 1.1, the image of $H^1(k, \mathbb{Z}_3)$ in L^*/L^{*3} consists of those $\overline{\xi}$ with $\sigma(\xi) = r^3\xi^{-1}$ for some $r \in L^*$. Since $\sigma(r^3) = r^3$, r can be chosen so that $r \in k^*$. For such a $\overline{\xi}$ the field extension of k associated to the inverse image of $\overline{\xi}$ in $H^1(k, \mathbb{Z}_3)$ is the field K with $K \cdot L = L(\sqrt[3]{\xi})$, which is described in Lemma 4.3. For $(r, s) \in \mathcal{E}(k)$, by definition of the map α in (3.10), $\partial(r, s) \in H^1(k, \mathcal{T}')$ maps to $\alpha(r, s) = \overline{s + \sqrt{c}}$ in L^*/L^{*3} (cf. Proposition 3.2). So, the associated cyclic field extension of k is the S of Lemma 4.3 lying in $L(\sqrt[3]{s + \sqrt{c}})$. Thus, by [Se, p. 204, Prop. 2], $\partial(r, s) \cup [\gamma_a]$ is the Brauer class of the cyclic algebra $(S/k, \tau, a)$, where τ is the restriction to S of the L-automorphism of $L(\sqrt[3]{s + \sqrt{c}})$ sending $\sqrt[3]{s + \sqrt{c}}$ to $\omega\sqrt[3]{s + \sqrt{c}}$. $\square$

Remark 4.5. Lemma 4.3 (ii) shows that if $(r,s) \in \mathcal{E}(k)$, then the corresponding field S is $k(u)$, where $u = \sqrt[3]{s+\sqrt{c}}\ + \sqrt[3]{s-\sqrt{c}}$, (with the cube roots chosen so that their product is r); the minimal polynomial of u over k is $min(u,k) = X^3 - 3rX - 2s$. Note that this minimal polynomial has discriminant $-4(-3r)^3 - 27(-2s)^2 = 4{\cdot}27(r^3 - s^2) = 27^2a^2b^2$, which is a square in k. Thus, the Galois group of the splitting field S of $min(u,k)$ over k must be cyclic of order 3.

Corollary 4.6. *Let $\mathcal{C}\colon Z^3 = aX^3 + bY^3$, $a,b \in k^*$, be a curve over k, and $\mathcal{E}$ the Jacobian of $\mathcal{C}$. For the map $\alpha\colon \mathcal{E}(k) \to k(\sqrt{c})^*/k(\sqrt{c})^{*3}$ in* (3.9)*, if $im(\alpha)$ is trivial, then $Br(k(\mathcal{C})/k) = \{\,0\,\}$.*

Proof. The definition of α shows that if α is trivial, then so is the connecting homomorphism $\partial\colon \mathcal{E}(k) \to H^1(k,\mathcal{T}')$. When this occurs, the epimorphism $\beta\colon \mathcal{E}(k) \to Br(k(\mathcal{C})/k)$ of (4.4) is clearly also trivial, and so its image must be trivial. □

§5. $Br(k(C)/k)$ for k a global field with specific examples, diagonal case

In this section, we study various useful facts on elliptic curves of the form $\mathcal{E}\colon Y^2 = X^3 + c$, which are Jacobians of curves $\mathcal{C}\colon Z^2 = f(X,Y)$ where $f(X,Y)$ is a binary cubic form. Based on these facts, we give assorted examples of relative Brauer groups $Br(k(\mathcal{C})/k)$ where $\mathcal{C}$ is a diagonal cubic curve $Z^3 = aX^3 + bY^3$ over $k = \mathbb{Q}$ or $\mathbb{Q}(\omega)$. Examples of nondiagonal case will be given at the end of §6.

Lemma 5.1. *Let $\lambda\colon A \to B$ and $\lambda'\colon B \to C$ be group homomorphisms such that the kernels and cokernels of λ and λ' are all finite. Then $ker\,(\lambda'\circ\lambda)$ and $coker\,(\lambda'\circ\lambda)$ are finite, and*

$$\frac{\bigl|coker\,(\lambda'\circ\lambda)\bigr|}{\bigl|ker\,(\lambda'\circ\lambda)\bigr|} = \frac{\bigl|coker\,(\lambda')\bigr|\cdot\bigl|coker\,(\lambda)\bigr|}{\bigl|ker\,(\lambda')\bigr|\cdot\bigl|ker\,(\lambda)\bigr|}. \tag{5.1}$$

Proof. It is easy to check that there is is an exact sequence with the obvious maps (cf. [Mi, Lemma A.2, p. 86]),

$$0 \to ker(\lambda) \to ker(\lambda'\circ\lambda) \to ker(\lambda') \to coker(\lambda) \to coker(\lambda'\circ\lambda) \to coker(\lambda') \to 0.$$

Since the kernels and cokernels of λ and λ' are all assumed to be finite, it is easy to check (or see [Mi, Lemma 3.7, p. 79]) that

$$\bigl|ker(\lambda)\bigr|\,\bigl|ker(\lambda')\bigr|\,\bigl|coker(\lambda'\circ\lambda)\bigr| = \bigl|ker(\lambda'\circ\lambda)\bigr|\,\bigl|coker\,(\lambda)\bigr|\,\bigl|coker\,(\lambda')\bigr|.$$

This yields the formula in (5.1). □

Let $\mathcal{E}\colon Y^2 = X^3 + c$ and $\mathcal{E}'\colon Y^2 = X^3 + d$, where $d = -27c \in k^*$, be elliptic curves over k. Recall that the *rank* of $\mathcal{E}(k)$, call it g, is the rank torsion-free of $\mathcal{E}(k)$, i.e., $g = dim_{\mathbb{Q}}(\mathcal{E}(k) \otimes_{\mathbb{Z}} \mathbb{Q})$. Notice that $\mathcal{E}(k)$ and $\mathcal{E}'(k)$ have the same rank since they are isogenous.

In Lemma 5.1, if we put $A = C = \mathcal{E}(k)$ and $B = \mathcal{E}'(k)$, we have

Proposition 5.2. *Let k be a global field. Let λ, λ' be the maps as in* (3.1), (3.2)*, the map α as in Proposition 3.2, and the map α' analogous to α, d replacing c. If $\mathcal{E}(k)$ has rank g, then*

$$3^g = \frac{\bigl|im\,(\alpha)\bigr|\cdot\bigl|im\,(\alpha')\bigr|}{\bigl|ker\,(\lambda')\bigr|\cdot\bigl|ker\,(\lambda)\bigr|}.$$

Proof. By the Mordell-Weil Theorem, one has $\mathcal{E}(k) \cong (\bigoplus_{j=1}^{g} \mathbb{Z}) \bigoplus (\bigoplus_{i=1}^{\ell} \mathbb{Z}_{p_i^{n_i}})$, and so

$$\mathcal{E}(k)/3\mathcal{E}(k) \;\cong\; (\bigoplus_{j=1}^{g} \mathbb{Z}/3\mathbb{Z}) \bigoplus (\bigoplus_{i=1}^{\ell} \mathbb{Z}_{p_i^{n_i}}/3\mathbb{Z}_{p_i^{n_i}}).$$

If the prime p_i is different from 3, then $\mathbb{Z}_{p_i^{n_i}}/3\mathbb{Z}_{p_i^{n_i}} = 0$. On the other hand, since $\mathbb{Z}_{3^{n_i}}/3\mathbb{Z}_{3^{n_i}} \cong \mathbb{Z}/3\mathbb{Z}$, it follows that

$$[\mathcal{E}(k) : 3\mathcal{E}(k)] \;=\; 3^{g+t}$$

where t is the number of i with $p_i = 3$. If $\mathcal{E}(k)_3$ denotes the 3-torsion subgroup of $\mathcal{E}(k)$, then $|\mathcal{E}(k)_3| = 3^t$ and thus

$$[\mathcal{E}(k) : 3\mathcal{E}(k)] \;=\; 3^g \cdot |\mathcal{E}(k)_3|. \tag{5.2}$$

Now, since $\big|coker\,(\lambda'\circ\lambda)\big| = \big|\mathcal{E}(k)/3\mathcal{E}(k)\big| = [\mathcal{E}(k):3\mathcal{E}(k)]$ and $\big|ker\,(\lambda'\circ\lambda)\big| = \big|\mathcal{E}(k)_3\big|$, it follows from (5.2) that $\dfrac{\big|coker\,(\lambda'\circ\lambda)\big|}{\big|ker\,(\lambda'\circ\lambda)\big|} = 3^g$. On the other hand, we have

$$coker\,(\lambda') \;=\; \mathcal{E}(k)/im(\lambda') \;\cong\; \mathcal{E}(k)/ker(\alpha) \;\cong\; im(\alpha).$$

and analogously $coker\,(\lambda) \cong im(\alpha')$. This completes the proof. $\square$

The following corollary describes the relationship between the rank g of $\mathcal{E}(k)$ and the images of the maps α and α' respectively. This observation leads us to investigate effectively the structure of the relative Brauer groups of binary cubic curves as we will see later. Notice that $\sqrt{c} \notin k$, $\sqrt{d} \in k$ is equivalent to $c \in -3\,k^{*2}$, $\omega \notin k$, since $d = -27c$, and that $\sqrt{c}$, $\sqrt{d} \in k$ is equivalent to $\sqrt{c}$, $\omega \in k$.

Corollary 5.3. *Let k be a global field. Let $\mathcal{E}\colon Y^2 = X^3 + c$ and $\mathcal{E}'\colon Y^2 = X^3 + d$ be the elliptic curves over k, where $d = -27c \in k^*$, and let α, α' be the maps as above.*

(i) *If $\sqrt{c} \notin k$ but $\sqrt{d} \in k$ (so, $\omega \notin k$), then*

$$|im(\alpha)|\cdot|im(\alpha')| \;=\; 3^{g+1}. \tag{5.3}$$

If $\sqrt{c}, \sqrt{d}, \omega \notin k$, then

$$|im(\alpha)|\cdot|im(\alpha')| \;=\; 3^{g}. \tag{5.4}$$

(ii) *If $\sqrt{c}$, $\sqrt{d} \in k$ (so, $\omega \in k$), then*

$$|im(\alpha)\,| \;=\; 3^{(g+2)/2}. \tag{5.5}$$

If $\sqrt{c}, \sqrt{d} \notin k$ but $\omega \in k$, then

$$|im(\alpha)| \;=\; 3^{g/2}.$$

Proof. (i) This is obvious by counting the orders of $ker\,(\lambda')$ and $ker\,(\lambda)$, and applying Proposition 5.2.

(ii) We first show that if $\omega \in k$, then $im(\alpha) = im(\alpha')$. To see this, notice that the equation $s^2 = r^3 - 27c$ can be rewritten as $(\frac{s}{\sqrt{-3}^3})^2 = (\frac{r}{\sqrt{-3}^2})^3 + c$ since $-27 = \sqrt{-3}^6$. This observation provides an isomorphism $\mathcal{E}(k) \cong \mathcal{E}'(k)$, given by $(r, s) \mapsto (\sqrt{-3}^2 r, \sqrt{-3}^3 s)$. Moreover, we have

$$\alpha'\big(\sqrt{-3}^2 r, \sqrt{-3}^3 s\big) \;=\; \overline{\sqrt{-3}^3 s + \sqrt{-27c}} \;=\; \overline{s + \sqrt{c}} \;=\; \alpha(r, s).$$

This shows that $im(\alpha) = im(\alpha')$. Now, if $\sqrt{c}$, $\sqrt{d} \in k$, then $|ker\,(\lambda')|\cdot|ker\,(\lambda)| = 9$. Thus, by Proposition 5.2, we have $|im(\alpha)|^2/9 = 3^g$, which leads to (5.5). Similarly, if $\sqrt{c}$, $\sqrt{d} \notin k$, then $|im(\alpha)|^2 = 3^g$. This completes the proof. $\square$

Corollary 5.4. *Let k be a global field and let $\mathcal{E}\colon Y^2 = X^3 + c$ be the elliptic curve over k. If $\omega \in k$, then $\mathcal{E}(k)$ has even rank.*

For the following proposition, let k be a field with discrete valuation. For each prime spot $\mathfrak{p}$ of k, we denote by $v_\mathfrak{p}$ the normalized discrete valuation corresponding to $\mathfrak{p}$.

Proposition 5.5. *Let k be a field with discrete valuation. Assume that (r, s) is a k-rational point of the elliptic curve $\mathcal{E}\colon Y^2 = X^3 + n^2$, $n \in k^*$. Then, for each prime spot $\mathfrak{p}$ of k with $v_\mathfrak{p}(s+n) \not\equiv 0 \ (mod\, 3)$, one has $v_\mathfrak{p}(2n) \not\equiv 0 \ (mod\, 3)$.*

Proof. Since $r^3 = s^2 - n^2 = (s+n)(s-n)$, it follows that

$$v_\mathfrak{p}(s+n) + v_\mathfrak{p}(s-n) \equiv 0 \ (mod\, 3). \tag{5.6}$$

This implies that $v_\mathfrak{p}(s+n) \neq v_\mathfrak{p}(s-n)$ since $v_\mathfrak{p}(s+n) \not\equiv 0 \ (mod\ 3)$. Thus, we have $v_\mathfrak{p}(2n) = min\big(v_\mathfrak{p}(s+n), v_\mathfrak{p}(s-n)\big)$. Suppose now that $v_\mathfrak{p}(2n) \equiv 0 \ (mod\ 3)$. Then 3 divides one of $v_\mathfrak{p}(s+n)$ and $v_\mathfrak{p}(s-n)$ but in fact both because of (5.6). This contradicts the assumption that $v_\mathfrak{p}(s+n) \not\equiv 0 \ (mod\, 3)$. $\square$

Suppose k is the quotient field of a unique factorization domain R. For $a \in k^*$, we say that $b \in k^*$ is “the” third-power-free part of a if b is third-power-free in its prime factorization and $b \equiv a \ (\text{mod } k^{*3})$. So, b is unique up to $R^* \cap k^{*3}$. Proposition 5.5 shows that $im(\alpha)$ lies in the $\mathbb{Z}/3\mathbb{Z}$-vector subspace of k^*/k^{*3} generated by cube classes of units and all prime elements dividing the numerator or denominator of the third-power-free part of $2n$. In particular, we are most interested in the fields $\mathbb{Q}$ and $\mathbb{Q}(\omega)$, which are the quotient fields of unique factorization domains $\mathbb{Z}$ and $\mathbb{Z}[\omega]$ with units $\{\pm 1\}$ and $\{\pm 1, \pm\omega, \pm\omega^2\}$, respectively. Since $-1 \in \mathbb{Q}^{*3} \subseteq \mathbb{Q}(\omega)^{*3}$, we have

Corollary 5.6. *Let $\mathcal{E}\colon Y^2 = X^3 + n^2$, $n \in k^*$ be an elliptic curve over a field k. Then, $im(\alpha)$ lies in the $\mathbb{Z}/3\mathbb{Z}$-vector space generated by the following*:

(i) *all primes dividing the numerator or denominator of the third-power-free part of $2n$, if $k = \mathbb{Q}$.*
(ii) *ω and all primes dividing the numerator or denominator of the third-power-free part of $2n$, if $k = \mathbb{Q}(\omega)$.*

Consider the maps $\alpha\colon k \to k(\sqrt{c})^*/k(\sqrt{c})^{*3}$ and $\alpha'\colon k \to k(\sqrt{d})^*/k(\sqrt{d})^{*3}$. For $x = c$ or d, we note that the canonical map

$$i_x\colon k(\sqrt{x})^*/k(\sqrt{x})^{*3} \to k(\sqrt{c}, \sqrt{d})^*/k(\sqrt{c}, \sqrt{d})^{*3}$$

is injective. Thus, we will identify a cube class in $k(\sqrt{x})^*/k(\sqrt{x})^{*3}$ with its image under the map i_x and write $im(\alpha')$ for $im(i_x \circ \alpha')$ in $k(\sqrt{c}, \sqrt{d})^*/k(\sqrt{c}, \sqrt{d})^{*3}$ by abuse of notation.

Proposition 5.7. *Let k be a field which does not contain ω. Let $\mathcal{E}$ and $\mathcal{E}'$ be the elliptic curves over k given by $\mathcal{E}\colon Y^2 = X^3 + c$ and $\mathcal{E}'\colon Y^2 = X^3 + d$, where $d = -27c \in k^*$. Then*

$$im(\alpha) \cap im(\alpha') = \{\,\overline{1}\,\}.$$

Proof. Let $\overline{\xi} \in im(\alpha) \cap im(\alpha')$. Since $\overline{\xi} \in im(\alpha)$, ξ is of the form $s + \sqrt{c}$ for some (r, s) in $\mathcal{E}(k)$. Let $G = \mathcal{G}al(k(\sqrt{c}, \sqrt{d})/k)$ and take the $\sigma \in G$ with $\sqrt{c} \mapsto -\sqrt{c}$ but $\sqrt{d}$ fixed. Then, G acts on $k(\sqrt{c}, \sqrt{d})^*/k(\sqrt{c}, \sqrt{d})^{*3}$ and thus

$$\sigma(\overline{\xi}) = \overline{\sigma(s+\sqrt{c})} = \overline{s - \sqrt{c}} = \overline{s+\sqrt{c}}^{\,-1} = \overline{\xi}^{\,-1},$$

since $(s+\sqrt{c})(s-\sqrt{c}) = r^3$. On the other hand, since $\overline{\xi} \in im(\alpha')$, it follows that $\overline{\xi}$ is fixed under the map σ. In other words, $\overline{\xi} = \overline{\xi}^{\,-1}$, which implies that $\overline{\xi} = \overline{1}$. $\square$

Let M be a finitely generated abelian group. Recall that the rank of M is defined by $rank(M) = dim_{\mathbb{Q}}(M \otimes_{\mathbb{Z}} \mathbb{Q})$. Assume that G is a group of order 2 and that G acts on M (so M has a $\mathbb{Z}[G]$-module structure). Denote by M^G the submodule of M fixed under the action of G and by $\widetilde{M}^G$ the submodule of M fixed under the twisted action of G, that is, for the $\sigma \in G$, $\sigma \neq id$,

$$\widetilde{M}^G \;=\; \{\, m \in M \,|\, \sigma(m) = -m \,\}.$$

Lemma 5.8. *Let M be a finitely generated abelian group. With M^G and $\widetilde{M}^G$ as above, we have*

$$rank(M) \;=\; rank(M^G) + rank(\widetilde{M}^G).$$

Proof. Define

$$M_1 \;=\; \{\, m+\sigma(m) \,|\, m \in M \,\} \quad \text{and} \quad M_2 \;=\; \{\, m-\sigma(m) \,|\, m \in M \,\}.$$

It is easy to check that M_1 and M_2 are G-fixed submodules of M and that $M_1 \subseteq M^G$ and $M_2 \subseteq \widetilde{M}^G$. Since $2m = m+\sigma(m)+m-\sigma(m)$, it follows that $2M \subseteq M_1 + M_2 \subseteq M^G + \widetilde{M}^G \subseteq M$. Since $2M$ has the same rank as M, it is obvious that $M^G \oplus \widetilde{M}^G$ has the same rank as M. Now, note that $M^G \cap \widetilde{M}^G$ is the set of 2-torsion elements. Thus, $M^G \cap \widetilde{M}^G$ must be finite (as M is finitely generated) and $rank(M^G \cap \widetilde{M}^G) = 0$. From the fact that

$$rank(M^G + \widetilde{M}^G) + rank(M^G \cap \widetilde{M}^G) = rank(M^G) + rank(\widetilde{M}^G),$$

we obtain

$$rank(M) = rank(M^G + \widetilde{M}^G) = rank(M^G) + rank(\widetilde{M}^G). \quad \square$$

The following proposition plays an important role to explicitly describe the relative Brauer groups of binary cubic curves over $\mathbb{Q}(\omega)$. We give a short and direct proof of it though this result is already known (see [Gr, Lemma 16.1.1, p. 49]).

Proposition 5.9. *Let k be a global field which does not contain ω and let $L = k(\omega) = k(\sqrt{-3})$. Let $\mathcal{E}$ be the elliptic curve over k given by $\mathcal{E}\colon Y^2 = X^3 + c$. Then,*

$$rank(\mathcal{E}(L)) \;=\; 2\, rank(\mathcal{E}(k)).$$

Proof. Let $G = \mathcal{G}al(L/k)$. It is obvious that $\mathcal{E}(L)^G = \mathcal{E}(k)$. We claim that $\widetilde{\mathcal{E}(L)}^G \cong \mathcal{E}'(k)$. For this, take the $\sigma \in G$, $\sigma \neq id$. Since $\sigma(r,s) = -(r,s)$ for any $(r,s) \in \widetilde{\mathcal{E}(L)}^G$, it follows that $(\sigma(r), \sigma(s)) = (r, -s)$. This shows that $r \in k$ and $s \in \sqrt{-3}\,k$ and so we can find r', $s' \in k$ such that $r = r'/\sqrt{-3}^2$ and $s = s'/\sqrt{-3}^3$. Then, the condition $s^2 = r^3 + c$ is equivalent to $(s')^2 = (r')^3 - 27c$. Define a map

$$\varphi\colon \mathcal{E}'(k) \to \Big\{\, \big(\tfrac{r'}{\sqrt{-3}^2}, \tfrac{s'}{\sqrt{-3}^3}\big) \in \mathcal{E}(L) \,\Big|\, r', s' \in k \,\Big\} \cup \{\, \mathcal{O} \,\}$$

given by $\varphi\big((r',s')\big) = \big(\frac{r'}{\sqrt{-3}^2}, \frac{s'}{\sqrt{-3}^3}\big)$ and $\varphi(\mathcal{O}) = \mathcal{O}$. Obviously, the map φ is bijective and the codomain of φ is $\widetilde{\mathcal{E}(L)}^G$. Further, using the formula of the group operation $\oplus$ on $\mathcal{E}$ (cf. §2), a straightforward calculation shows that the map φ is a group homomorphism. Hence, we have $\widetilde{\mathcal{E}(L)}^G \cong \mathcal{E}'(k)$ as claimed. Now, since there exist only finitely many 2-torsion points, it follows from Lemma 5.8 that

$$rank(\mathcal{E}(L)) = rank(\mathcal{E}(L)^G) + rank(\widetilde{\mathcal{E}(L)}^G) = rank(\mathcal{E}(k)) + rank(\mathcal{E}'(k)) = 2\,rank(\mathcal{E}(k)).$$

Note here that $rank(\mathcal{E}(k)) = rank(\mathcal{E}'(k))$ since the curves $\mathcal{E}$ and $\mathcal{E}'$ are isogenous. This completes the proof. $\square$

Proposition 5.9 confirms that the ranks of the elliptic curves in our situation are always even as we have seen in Corollary 5.4.

Corollary 5.10. *Let k be a global field not containing ω, and let $L = k(\omega) = k(\sqrt{-3})$. Let $\mathcal{E}$ be the elliptic curve over k given by $\mathcal{E}\colon Y^2 = X^3 + c$. Then, as $\mathbb{Z}/3\mathbb{Z}$-vector spaces,*

$$dim\,\alpha(\mathcal{E}(L)) = dim\,\alpha(\mathcal{E}(k)) + dim\,\alpha'(\mathcal{E}'(k)).$$

Let $\mathcal{E}$ be the elliptic curve defined by $\mathcal{E}\colon Y^2 = X^3 + c$ over $\mathbb{Q}$, where c is a sixth-power-free integer. If $\mathcal{E}_{tors}(\mathbb{Q})$ denotes the torsion subgroup of $\mathcal{E}(\mathbb{Q})$, then it is known (cf. [Hu, Th. 3.3, p. 35]) that

$$\mathcal{E}_{tors}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } c = 1, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } c \neq 1 \text{ is a square, or } c = -432 = -2^4\cdot 3^3, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } c \neq 1 \text{ is a cube,} \\ \{\,\mathcal{O}\,\} & \text{otherwise.} \end{cases} \tag{5.7}$$

In the curve $\mathcal{E}$ above, we may assume that c is an integer because otherwise we can take an isomorphic curve by multiplying c by the sixth power of the denominator of c. We can now handle the rank 0 case completely.

Proposition 5.11. *For $a, b \in \mathbb{Q}^*$, let $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ be a projective curve over $\mathbb{Q}$, and let $\mathcal{E}\colon Y^2 = X^3 + c$ be the Jacobian of $\mathcal{C}$, where $c = -\frac{27}{4}a^2b^2$ is a sixth-power-free integer. Let $k = \mathbb{Q}(\omega)$.*

(i) *If $c = -432$, then $\mathcal{E}(\mathbb{Q})$ has rank 0 and*

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) = \langle\, [(\mathbb{Q}(u)/\mathbb{Q}, \tau, a)]\,\rangle \quad \text{and} \quad Br(k(\mathcal{C})/k) = \langle\, [(a,\omega)_\omega]\,\rangle,$$

where $u = \sqrt[3]{36 + 12\sqrt{-3}} + \sqrt[3]{36 - 12\sqrt{-3}}$, with the cube roots chosen so that their product is 12.

(ii) *If $\mathcal{E}(\mathbb{Q})$ has rank 0 and $c \neq -432$, then*

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) = \{\,0\,\} \ \ \text{while} \ \ Br(k(\mathcal{C})/k) = \langle\, [(a,b)_\omega]\,\rangle.$$

PROOF. Since $\mathcal{E}(\mathbb{Q})$ is assumed to have rank 0, we have $\mathcal{E}(\mathbb{Q}) = \mathcal{E}_{tors}(\mathbb{Q})$. According to (5.7), all possible cases of rank 0 with $c = -\frac{27}{4}a^2b^2$ can be represented as follows:

$$\mathcal{E}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } c = -432 = -2^4\cdot 3^3, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } c = -27, \\ \{\mathcal{O}\} & \text{otherwise.} \end{cases}$$

(i) If $c = -432$, then $\mathcal{E}(\mathbb{Q})$ indeed has rank 0 (cf. [SAGE] or see Remark 5.12 below) with rational points $(12, \pm 36)$ other than $\mathcal{O}$. A short calculation shows that

$$\alpha(12,36) = \overline{36 + \sqrt{-3^3\cdot 4^2}} = \overline{4\cdot 3\sqrt{-3}(-\sqrt{-3}+1)} = \overline{-2^3\cdot\sqrt{-3}^3(\tfrac{-1+\sqrt{-3}}{2})} = \overline{\omega}.$$

Since the point $(12,-36)$ is the inverse of $(12,36)$, we obviously have $\alpha(12,-36) = \overline{\omega^2}$, and thus $\alpha(\mathcal{E}(\mathbb{Q})) = \langle\omega\rangle$. Further, since $\mathcal{E}(k)$ also has rank 0 by Proposition 5.9, it follows from (5.5) that $\alpha(\mathcal{E}(k)) = \langle\omega\rangle$. Hence, by Propositions 4.1 and 4.4, we have

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) = \langle\, [(\mathbb{Q}(u)/\mathbb{Q}, \tau, a)]\,\rangle \quad \text{and} \quad Br(k(\mathcal{C})/k) = \langle\, [(a,\omega)_\omega]\,\rangle,$$

where $u = \sqrt[3]{36 + 12\sqrt{-3}} + \sqrt[3]{36 - 12\sqrt{-3}}$ for cube roots with product 12, by Remark 4.5.

(ii) If $c = -27$, then $\mathcal{E}(\mathbb{Q})$ has rank 0 (cf. [SAGE]). Since $\mathcal{E}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ but $\mathbb{Q}(\sqrt{c})^*/\mathbb{Q}(\sqrt{c})^{*3}$ is 3-torsion, we have $\alpha(\mathcal{E}(\mathbb{Q})) = \{\,\overline{1}\,\}$. If $\mathcal{E}(\mathbb{Q})$ has rank 0 with $c \neq -432$ or -27, then $\mathcal{E}(\mathbb{Q}) = \{\,\mathcal{O}\,\}$ by (5.7) and thus $\alpha(\mathcal{E}(\mathbb{Q})) = \{\,\overline{1}\,\}$. On the other hand, since $\mathcal{E}(k)$ also has rank 0 and contains two k-rational points $(0, \pm\sqrt{c})$ other than $\mathcal{O}$, it follows that $\alpha(\mathcal{E}(k)) = \langle\overline{2\sqrt{c}}\rangle$. Hence, by Corollary 4.6 and Remark 4.2 (i) respectively, we have

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) = \{0\} \quad \text{and} \quad Br(k(\mathcal{C})/k) = \langle\, [(a,b)_\omega]\,\rangle. \qquad \square$$

Remark 5.12. In Proposition 5.11 (i), we can show directly that the rank of $\mathcal{E}(\mathbb{Q})$ is 0. To show this, for the curve $\mathcal{E}\colon Y^2 = X^3 - 3^3\cdot 4^2$, consider the isogenous curve $\mathcal{E}'\colon Y^2 = X^3 + 4^2$. The image of the map $\alpha'\colon \mathcal{E}'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*3}$ must be trivial by Corollary 5.6 (i). On the other hand, in $k = \mathbb{Q}(\sqrt{-3})$, notice that $-3^3\cdot 4^2$ is a square and $\overline{2\cdot\sqrt{-3^3\cdot 4^2}} = \overline{1}$ in k^*/k^{*3}. By Corollary 5.6 (ii), we then have $\alpha(\mathcal{E}(k)) \subseteq \langle\,\overline{\omega}\,\rangle$. Since $\mathcal{E}(\mathbb{Q}) \subseteq \mathcal{E}(k)$, it follows that $\alpha(\mathcal{E}(\mathbb{Q})) \subseteq \langle\,\overline{\omega}\,\rangle$. Thanks to the formula in (5.3), the rank of $\mathcal{E}(\mathbb{Q})$ must be 0.

For the rest of this section, we provide various examples of relative Brauer groups of function fields of diagonal cubic forms. For a curve $\mathcal{E}\colon Y^2 = X^3 + c$, we may take as its isogenous curve $\mathcal{E}'\colon Y^2 = X^3 - \frac{c}{27}$ instead of $Y^2 = X^3 - 27c$ since these two curves are isomorphic.

Example 5.13. Consider the projective curve $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ $(a, b \in \mathbb{Q}^*)$ with $ab = 2\cdot 11$. The Jacobian of $\mathcal{C}$ is $\mathcal{E}\colon Y^2 = X^3 - 27\cdot 11^2$ and its isogenous curve is $\mathcal{E}'\colon Y^2 = X^3 + 11^2$. It is known (cf. [SAGE]) that the curve $\mathcal{E}'$ (so $\mathcal{E}$ as well) has rank 1. Notice that $\mathcal{E}'$ has integer points $(0, 11)$, $(12, 43)$, which are sufficient to determine $\alpha(\mathcal{E}(\mathbb{Q}))$ and $\alpha'(\mathcal{E}'(\mathbb{Q}))$. The images of these points in $\mathbb{Q}^*/\mathbb{Q}^{*3}$ are $\overline{2\cdot 11}$, $\overline{2\cdot 27}\ (= \overline{2})$. Since $\alpha'(\mathcal{E}'(\mathbb{Q}))$ is contained in the $\mathbb{Z}/3\mathbb{Z}$-vector space generated by all primes dividing the third-power-free part of $2n$ by Corollary 5.6 (i), it follows that $\alpha'(\mathcal{E}'(\mathbb{Q})) = \langle\,\overline{2}, \overline{11}\,\rangle$. Then, the formula in (5.3) with the rank information implies that $\alpha(\mathcal{E}(\mathbb{Q})) = \{\,\overline{1}\,\}$. Hence, by Corollary 4.6, we have

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) = \{\,0\,\}.$$

For $k = \mathbb{Q}(\omega)$, we next consider the curves $\mathcal{E}$ and $\mathcal{E}'$ over k. Note that the primes 2 and 11 are unramified in k. Since the two integer points of the curve $\mathcal{E}'$ above again have images $\overline{2\cdot 11}$, $\overline{2}$ in k^*/k^{*3}, this implies that $\langle\, \overline{2}, \overline{11}\,\rangle \subseteq \alpha(\mathcal{E}(k)) \subseteq \langle\, \overline{\omega}, \overline{2}, \overline{11}\,\rangle$. However, since $\mathcal{E}(k)$ has rank 2 by Proposition 5.9, it follows that $\alpha(\mathcal{E}(k)) = \langle\, \overline{2}, \overline{11}\,\rangle$ and

$$Br(k(\mathcal{C})/k) \;=\; \langle\, [(a,2)_\omega],\, [(a,11)_\omega]\,\rangle.$$

This is valid for any choice of $a \in \mathbb{Q}^*$ when we set $b = 22/a$. Clearly $\big|Br(k(\mathcal{C})/k)\big|$ depends on the choice of a.

For a specific example, let $a = 2$ (and so $b = 11$). Note that $(2,2)_\omega \cong (2,-1)_\omega$ is obviously split and that $(2,11)_\omega$ is also split since 11 is a norm for the extension $k(\sqrt[3]{2})/k$, as $11 = 3^3 - 2\cdot 2^3$. Hence, we have

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) \;=\; Br(k(\mathcal{C})/k) \;=\; \{\,0\,\}.$$

Example 5.14. Consider the projective curve $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ with $ab = 2\cdot 3\cdot 5$. The Jacobian of $\mathcal{C}$ is $\mathcal{E}\colon Y^2 = X^3 - 27\cdot 15^2$ and its isogenous curve is $\mathcal{E}'\colon Y^2 = X^3 + 15^2$. It is known (cf. [SAGE]) that the curve $\mathcal{E}'$ has rank 2. Notice that $\mathcal{E}'$ has integer points $(-5,-10)$, $(0,15)$, $(4,-17)$, whose images in $\mathbb{Q}^*/\mathbb{Q}^{*3}$ are $\overline{5}$, $\overline{30}\,(=\overline{2\cdot 3\cdot 5})$, $\overline{-2}\,(=\overline{2})$, respectively. Then, Corollary 5.6 (i) tells us that $\alpha'(\mathcal{E}'(\mathbb{Q})) = \langle\, \overline{2}, \overline{3}, \overline{5}\,\rangle$. Thanks to the formula in (5.3), we have $\alpha(\mathcal{E}(\mathbb{Q})) = \{\,\overline{1}\,\}$. Hence, by Corollary 4.6,

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) \;=\; \{\,0\,\}.$$

Next, we observe that the primes 2 and 5 are unramified and 3 is ramified in $k = \mathbb{Q}(\sqrt{-3})$ (note that $\sqrt{-3}$ is the prime of k above 3). The three integer points of the curve $\mathcal{E}'$ above again have images $\overline{5}$, $\overline{30}$, $\overline{2}$ in k^*/k^{*3} respectively. Since $30 = 2\cdot\sqrt{-3}^{\,2}\cdot 5$, it follows from Corollary 5.6 (ii) that

$$\langle\, \overline{2}, \overline{\sqrt{-3}}, \overline{5}\,\rangle \;\subseteq\; \alpha(\mathcal{E}(k)) \;=\; \alpha'(\mathcal{E}'(k)) \;\subseteq\; \langle\, \overline{\omega}, \overline{2}, \overline{\sqrt{-3}}, \overline{5}\,\rangle.$$

Since $\mathcal{E}(\mathbb{Q})$ has rank 2, it follows from Proposition 5.9 that $\mathcal{E}(k)$ has rank 4. Hence, we have $\alpha(\mathcal{E}(k)) = \langle\, \overline{2}, \overline{\sqrt{-3}}, \overline{5}\,\rangle$ and

$$Br(k(\mathcal{C})/k) \;=\; \langle\, [(a,2)_\omega],\, [(a,\sqrt{-3})_\omega],\, [(a,5)_\omega]\,\rangle.$$

Example 5.15. Take for $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ with $ab = 2\cdot 13$. The Jacobian of $\mathcal{C}$ is $\mathcal{E}\colon Y^2 = X^3 - 27\cdot 13^2$ and its isogenous curve is $\mathcal{E}'\colon Y^2 = X^3 + 13^2$. By [SAGE], we see that the curve $\mathcal{E}'$ has rank 1. Further, it can be checked that $\mathcal{E}$ and $\mathcal{E}'$ have integer points $(39, 234)$ and $(0, 13)$, respectively. Note that 13 is split in $k = \mathbb{Q}(\omega)$; in fact, $13 = \mathfrak{p}\mathfrak{q}$ where $\mathfrak{p} = 1 + 2\sqrt{-3}$ and $\mathfrak{q} = 1 - 2\sqrt{-3}$. We now claim that $\alpha(\mathcal{E}(\mathbb{Q})) = \langle\, \overline{\mathfrak{p}\mathfrak{q}^2}\,\rangle$. To see this, observe that

$$234 + \sqrt{-27\cdot 13^2} \;=\; 3\cdot 13\cdot\sqrt{-3}(-2\sqrt{-3}+1) \;=\; -\sqrt{-3}^{\,3}\cdot 13\cdot(1-2\sqrt{-3}) \;=\; -\sqrt{-3}^{\,3}\cdot\mathfrak{p}\mathfrak{q}^2.$$

Since $-\sqrt{-3}^{\,3}$ is a cube in k, it follows that $\langle\, \overline{\mathfrak{p}\mathfrak{q}^2}\,\rangle \subseteq \alpha(\mathcal{E}(\mathbb{Q}))$. On the other hand, we know $\langle\, \overline{2\cdot 13}\,\rangle \subseteq \alpha'(\mathcal{E}'(\mathbb{Q}))$. However, since the rank of the curve $\mathcal{E}$ is 1, it follows from the formula in (5.3) that

$$\alpha(\mathcal{E}(\mathbb{Q})) \;=\; \langle\, \overline{\mathfrak{p}\mathfrak{q}^2}\,\rangle \;\cong\; \mathbb{Z}/3\mathbb{Z} \quad\text{and}\quad \alpha'(\mathcal{E}'(\mathbb{Q})) \;=\; \langle\, \overline{2\cdot 13}\,\rangle \;\cong\; \mathbb{Z}/3\mathbb{Z}.$$

Hence, by Proposition 4.4,

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) \;=\; \langle\, [(\mathbb{Q}(u)/\mathbb{Q}, \tau, a)]\,\rangle$$

where $u = \sqrt[3]{234+39\sqrt{-3}} + \sqrt[3]{234-39\sqrt{-3}}$, with cube roots chosen so that their product is 39. Note here that $(\mathbb{Q}(u)/\mathbb{Q},\tau,a)\otimes_{\mathbb{Q}} k \cong (a,\mathfrak{p}\mathfrak{q}^2)_\omega$.

Next, over k, we have $\langle\, \overline{2\mathfrak{p}^2}, \overline{2\mathfrak{q}^2}\,\rangle \subseteq \alpha(\mathcal{E}(k)) \subseteq \langle\, \overline{\varpi},\, \overline{2},\, \overline{\mathfrak{p}},\, \overline{\mathfrak{q}}\,\rangle$. However, since $\mathcal{E}(k)$ has rank 2 by Proposition 5.9, we have $\alpha(\mathcal{E}(k)) = \langle\, \overline{2\mathfrak{p}^2}, \overline{2\mathfrak{q}^2}\,\rangle$ and thus

$$Br(k(\mathcal{C})/k) \,=\, \langle\, [(a,2\mathfrak{p}^2)_\omega],\, [(a,2\mathfrak{q}^2)_\omega]\,\rangle.$$

For a specific example, let $a=3$, so we have $\mathcal{C}\colon Z^3 = 3X^3 + \frac{2\cdot 13}{3}Y^3$. In what follows, we describe the nonsplit algebras in the relative Brauer groups by means of local invariants. For this, it suffices to consider the symbol algebras over k locally at the prime spots 2, $\sqrt{-3}$, $\mathfrak{p}$, and $\mathfrak{q}$, where $\mathfrak{p}\cdot\mathfrak{q} = 13$. First, over the dyadic completion $\widehat{k}_2$, the symbol algebra $(3,2\mathfrak{p}^2;\widehat{k}_2)_\omega \cong (3,2;\widehat{k}_2)_\omega$ is split since 3 is a cube modulo 2 and by Hensel's lemma. Next, it is obvious that the invariant of $(3,2\mathfrak{p}^2;\widehat{k}_{\mathfrak{q}})_\omega$ at $\mathfrak{q}$, denoted $inv_{\mathfrak{q}}(3,2\mathfrak{p}^2;\widehat{k}_{\mathfrak{q}})_\omega$, is trivial in $\mathbb{Q}/\mathbb{Z}$ since 2, 3, and $\mathfrak{p}$ are units $\mathfrak{q}$-adically. In order to determine $inv_{\mathfrak{p}}(3,2\mathfrak{p}^2;\widehat{k}_{\mathfrak{p}})_\omega$, consider the algebra $(3,\mathfrak{p};\widehat{k}_{\mathfrak{p}})_\omega$. Since 13 is split in k, notice that $\widehat{k}_{\mathfrak{p}} = \widehat{\mathbb{Q}}_{13}$ and the residue field $\overline{k}_{\mathfrak{p}} = \mathbb{Z}_{13}$. Inside the algebra, we have defining relations $i^3 = 3$, $j^3 = \mathfrak{p}$, $ij = \omega ji$. From the unramified extension $\widehat{k}_{\mathfrak{p}}(i)/\widehat{k}_{\mathfrak{p}}$ of degree 3, we consider the induced automorphism φ of the residue field $\mathbb{Z}_{13}(\overline{\imath})$, which is some power of the Frobenius automorphism. Since $\mathfrak{p} = 1+2\sqrt{-3}$, it follows that $\sqrt{-3} \equiv \frac{-1}{2}$ $(mod\ \mathfrak{p})$. Observing that $\overline{\varpi} = \overline{(-1+\sqrt{-3})\,/\,2} = \overline{(-1-(1/2))\,/\,2} = \overline{-3/4} = \overline{3^2}$ in $\mathbb{Z}_{13}$ and so $\overline{\omega^{-1}} = \overline{3}$, we have $\varphi(\overline{\imath}) = \overline{jij^{-1}} = \overline{\omega^{-1}i} = \overline{3i} = \overline{\imath}^{13}$. Therefore the map φ, conjugation by $\overline{\jmath}$, is the Frobenius automorphism and so $inv_{\mathfrak{p}}(3,2\mathfrak{p}^2;\widehat{k}_{\mathfrak{p}})_\omega = \overline{2/3}$. By Hilbert's Reciprocity Law, the symbol algebra $(3,2\mathfrak{p}^2;k)_\omega$ has local invariant $\frac{2}{3}$ at $\mathfrak{p}$, $\frac{1}{3}$ at $\sqrt{-3}$, and 0 at all other prime spots. By similar calculations, it can be shown that the algebra $(3,2\mathfrak{q}^2;k)_\omega$ has local invariant $\frac{1}{3}$ at $\mathfrak{q}$, $\frac{2}{3}$ at $\sqrt{-3}$, and 0 at all other prime spots. As $(3,\mathfrak{p}\mathfrak{q}^2)_\omega \sim (3,2\mathfrak{p}^2)^2_\omega \otimes_k (3,2\mathfrak{q}^2)_\omega$, the algebra $(3,\mathfrak{p}\mathfrak{q}^2)_\omega$ has local invariant $\frac{1}{3}$ at each of $\mathfrak{p}$, $\mathfrak{q}$, and $\sqrt{-3}$. Consequently, the cyclic algebra $A := (\mathbb{Q}(u)/\mathbb{Q},\tau,2)$ satisfying $A\otimes_{\mathbb{Q}} k \cong (a,\mathfrak{p}\mathfrak{q}^2)_\omega$ has local invariant $\frac{1}{3}$ at 13 and $\frac{2}{3}$ at 3, and 0 at other prime spots.

Example 5.16. Consider $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ with $ab = 136 = 2^3\cdot 17$. The Jacobian of $\mathcal{C}$ is $\mathcal{E}\colon Y^2 = X^3 - 27\cdot(4\cdot 17)^2$ and its isogenous curve is $\mathcal{E}'\colon Y^2 = X^3 + (4\cdot 17)^2$. In this example, we can easily show that the rank of $\mathcal{E}(k)$ is 2 (so, the rank of $\mathcal{E}(\mathbb{Q})$ is 1). Notice that $\mathcal{E}$ and $\mathcal{E}'$ have integer points $(84,684)$ and $(0,68)$, respectively, and that 17 is unramified in k. Since $2{\cdot}68 = 2^3{\cdot}17$, it follows from Corollary 5.6 (i) that $\alpha'(\mathcal{E}'(\mathbb{Q})) = \langle\, \overline{17}\,\rangle$. On the other hand, observe that

$$684+\sqrt{-27\cdot 4^2\cdot 17^2} \;=\; 3\sqrt{-3}\cdot 4(-19\sqrt{-3}+17) \;=\; \sqrt{-3}^3\cdot 2^3\cdot\tfrac{19\sqrt{-3}-17}{2} \;=\; -\sqrt{-3}^3\cdot 2^3\cdot(2-\sqrt{-3})^3\omega^2.$$

In other words, $\overline{684+\sqrt{-27\cdot 4^2\cdot 17^2}} = \overline{\omega^2}$, so $\langle\, \overline{\varpi}\,\rangle \subseteq \alpha(\mathcal{E}(\mathbb{Q}))$, which shows that $\alpha(\mathcal{E}(k)) = \langle\, \overline{\varpi},\, \overline{17}\,\rangle$ by Corollary 5.6 (ii). Therefore, the rank of $\mathcal{E}(k)$ must be 2 by the formula in (5.5). Since $\overline{17} \notin \mathcal{E}(\mathbb{Q})$ by Proposition 5.7, we have $\alpha(\mathcal{E}(\mathbb{Q})) = \langle\, \overline{\varpi}\,\rangle$. Hence, we have,

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) \,=\, \langle\, [(\mathbb{Q}(u)/\mathbb{Q},\tau,a)]\,\rangle$$

where $u = \sqrt[3]{684+204\sqrt{-3}} + \sqrt[3]{684-204\sqrt{-3}}$, with cube roots chosen so that their product is 84. Note here that $(\mathbb{Q}(u)/\mathbb{Q},\tau,a)\otimes_{\mathbb{Q}} k \cong (a,\omega)_\omega$. Moreover, we have

$$Br(k(\mathcal{C})/k) \,=\, \langle\, [(a,\omega)_\omega],\, [(a,b)_\omega]\,\rangle,$$

since $(a,17)_\omega \cong (a,b)_\omega$.

Example 5.17. Consider $\mathcal{C}\colon Z^3 = aX^3 + bY^3$ with $ab = 728 = 2^3{\cdot}7{\cdot}13$. The Jacobian of $\mathcal{C}$ is $\mathcal{E}\colon Y^2 = X^3 - 27(4{\cdot}7{\cdot}13)^2$ and its isogenous curve is $\mathcal{E}'\colon Y^2 = X^3 + (4{\cdot}7{\cdot}13)^2$. It is known (cf. [SAGE]) that the curve $\mathcal{E}$ has rank 2 over $\mathbb{Q}$. Also, $\mathcal{E}$ has rational points $(156, 468)$ and $(196, 1988)$ (found by computer search) and $\mathcal{E}'$ has rational point $(0, 364)$. Note that both 7 and 13 are split in $k = \mathbb{Q}(\omega)$; in fact, $7 = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 = 2 + \sqrt{-3}$ and $\mathfrak{p}_2 = 2 - \sqrt{-3}$, and $13 = \mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{q}_1 = 1 + 2\sqrt{-3}$ and $\mathfrak{q}_2 = 1 - 2\sqrt{-3}$. Since $2{\cdot}364 = 2^3{\cdot}7{\cdot}13$, it follows that $\langle\, \overline{7{\cdot}13}\,\rangle \subseteq \alpha'(\mathcal{E}'(\mathbb{Q}))$ by Corollary 5.6 (i). On the other hand, observe that

$$468 + \sqrt{-27(4{\cdot}7{\cdot}13)^2} \;=\; 4{\cdot}9{\cdot}13 + 4{\cdot}3{\cdot}7{\cdot}13\sqrt{-3} \;=\; 2^3{\cdot}\sqrt{-3}^{\,3}{\cdot}13{\cdot}\frac{\sqrt{-3}-7}{2} \;=\; 2^3{\cdot}\sqrt{-3}^{\,3}{\cdot}13\mathfrak{q}_2\omega^2.$$

Similarly, it can be shown that $1988 + \sqrt{-27(4{\cdot}7{\cdot}13)^2} = 2^3\mathfrak{p}_1^5\mathfrak{p}_2\omega^2$. So, $\langle\, \overline{\mathfrak{q}_1\mathfrak{q}_2^2\omega^2},\, \overline{\mathfrak{p}_1^2\mathfrak{p}_2\omega^2}\rangle \subseteq \alpha(\mathcal{E}(\mathbb{Q}))$. Since the rank of $\mathcal{E}(\mathbb{Q})$ is 2, the formula in (5.3) shows that $\alpha(\mathcal{E}(\mathbb{Q})) = \langle\, \overline{\mathfrak{q}_1\mathfrak{q}_2^2\omega^2},\, \overline{\mathfrak{p}_1^2\mathfrak{p}_2\omega^2}\rangle$. Likewise, since the rank of $\mathcal{E}(k)$ is 4, we have $\alpha(\mathcal{E}(k)) = \langle\, \overline{7{\cdot}13},\, \overline{\mathfrak{p}_1^2\mathfrak{p}_2\omega^2},\, \overline{\mathfrak{q}_1\mathfrak{q}_2^2\omega^2}\rangle$ by (5.5).

Hence, we conclude that

$$Br(\mathbb{Q}(\mathcal{C})/\mathbb{Q}) = \big\langle\, [(\mathbb{Q}(u_1)/\mathbb{Q}, \tau_1, a)], [(\mathbb{Q}(u_2)/\mathbb{Q}, \tau_2, a)]\,\big\rangle$$

where

$$u_1 \;=\; \sqrt[3]{468 + 1092\sqrt{-3}} + \sqrt[3]{468 - 1092\sqrt{-3}} \quad\text{and}\quad u_2 \;=\; \sqrt[3]{1988 + 1092\sqrt{-3}} + \sqrt[3]{1988 - 1092\sqrt{-3}}\,.$$

The cube roots in the formula for u_1 are chosen so that their product is real; likewise for u_2. Also, the automorphisms τ_1 and τ_2 are chosen so that $(\mathbb{Q}(u_1)/\mathbb{Q}, \tau_1, a) \otimes_{\mathbb{Q}} k \cong (a, \mathfrak{p}_1^2\mathfrak{p}_2\omega^2)_\omega$ and $(\mathbb{Q}(u_2)/\mathbb{Q}, \tau_2, a) \otimes_{\mathbb{Q}} k \cong (a, \mathfrak{q}_1\mathfrak{q}_2^2\omega^2)_\omega$. Furthermore, we have

$$Br(k(\mathcal{C})/k) = \langle\, [(a, 7{\cdot}13)_\omega], [(a, \mathfrak{p}_1^2\mathfrak{p}_2\omega^2)_\omega],\; [(a, \mathfrak{q}_1\mathfrak{q}_2^2\omega^2)_\omega]\,\rangle.$$

§6. The nondiagonal case

Let $\mathcal{C} = \mathcal{C}_f$ be the smooth projective genus 1 curve given by

$$\mathcal{C}_f\colon Z^3 \;=\; f(X,Y) \quad\text{where}\quad f(X,Y) \;=\; AX^3 + 3BX^2Y + 3CXY^2 + DY^3, \tag{6.1}$$

with $A, B, C, D \in k$. In previous sections, we have described the relative Brauer groups $Br(k(\mathcal{C})/k)$ in the diagonal case, that is, when $B = C = 0$. We now turn to the nondiagonal case.

If f is diagonalizable by a linear change of variables over k, then we can apply the diagonal case to compute $Br(k(\mathcal{C})/k)$. We recall when such a diagonalization is possible, following the approach in [D, pp. 16-17].

The Hessian matrix of f is

$$H_f(X,Y) \;=\; \begin{pmatrix} \partial^2 f/\partial X^2 & \partial^2 f/\partial X\,\partial Y \\ \partial^2 f/\partial Y\partial X & \partial^2 f/\partial Y^2 \end{pmatrix} \;=\; 6\begin{pmatrix} AX+BY & BX+CY \\ BX+CY & CX+DY \end{pmatrix}.$$

The Hessian determinant of f is defined to be

$$h_f(X,Y) \;=\; det\big(H_f(X,Y)\big) \;=\; 36(RX^2 + 2SXY + TY^2),$$

where

$$R \;=\; AC - B^2, \quad 2S \;=\; AD - BC, \quad \text{and} \quad T \;=\; BD - C^2. \tag{6.2}$$

The discriminant Δ_f of f is $\frac{1}{72^2}\cdot$(discriminant of h_f), that is,

$$\Delta_f \;=\; S^2 - RT \;=\; \tfrac{1}{4}\big(A^2D^2 - 3B^2C^2 + 4AC^3 + 4B^3D - 6ABCD\big). \tag{6.3}$$

$\big($Note that Δ_f is not the discriminant of the cubic polynomial $f(X,1) \in k[X]$. Indeed, $\Delta_f = \frac{-1}{4\cdot 27}\, disc\,(f(X,1)) \equiv -3\, disc\,(f(X,1)) \;(mod\; k^{*2})$.$\big)$ We assume throughout that f is nondegenerate, that is, $\Delta_f \neq 0$. This is equivalent to the condition that $f(X,1)$ has 3 distinct roots in an algebraic closure of k.

A short computation shows that f is diagonal (i.e., $B = C = 0$) if and only if $R = T = 0$. In this case, $\Delta_f = (AD/2)^2 \in k^{*2}$. We can use this to see that f is diagonalizable over k if and only if the quadratic form $h_f(X,Y)$ is isotropic over k, that is, if and only if its discriminant, Δ_f, is a square in k: Given new variables U and V, we set $X(U,V) = \alpha U + \beta V$ and $Y(U,V) = \gamma U + \delta V$ with $\alpha, \beta, \gamma, \delta \in k$ chosen so that the matrix $Q = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ satisfies $det(Q) \neq 0$. Let $\epsilon = det(Q)$. Then, for $\widetilde{f}(U,V) = f(X(U,V), Y(U,V))$, the chain rule yields

$$H_{\widetilde{f}}(U,V) \;=\; Q^t\, H_f(X(U,V), Y(U,V))\, Q.$$

Hence, $h_{\widetilde{f}}(U,V) = \epsilon^2 h_f(X(U,V), Y(U,V))$. If we write

$$h_f \;=\; 36(RX^2 + 2SXY + TY^2) \;=\; 36(\overline{R}U^2 + 2\overline{S}UV + \overline{T}V^2),$$

then

$$\begin{pmatrix} \overline{R} & \overline{S} \\ \overline{S} & \overline{T} \end{pmatrix} \;=\; Q^t \begin{pmatrix} R & S \\ S & T \end{pmatrix} Q,$$

and thus $\overline{R}\,\overline{T} - \overline{S}^2 = \epsilon^2(RT - S^2)$. By expressing $h_{\widetilde{f}} = 36(\widetilde{R}U^2 + 2\widetilde{S}UV + \widetilde{T}V^2)$, since $h_{\widetilde{f}}(U,V) = \epsilon^2 h_f(X(U,V), Y(U,V))$, it follows that $\widetilde{R} = \epsilon^2\overline{R}$, $\widetilde{S} = \epsilon^2\overline{S}$, and $\widetilde{T} = \epsilon^2\overline{T}$. Hence,

$$\Delta_{\widetilde{f}} \;=\; \widetilde{S}^2 - \widetilde{R}\widetilde{T} \;=\; \epsilon^4(\overline{S}^2 - \overline{R}\,\overline{T}) \;=\; \epsilon^6\Delta_f.$$

Thus, if $\Delta_f \notin k^{*2}$, then $\Delta_{\widetilde{f}} \notin k^{*2}$ and so $\widetilde{f}$ is not diagonal over k. Conversely, suppose that $\Delta_f \in k^{*2}$ but f is not diagonal (so $R \neq 0$ or $T \neq 0$). If $R \neq 0$, we have

$$h_f \;=\; \tfrac{36}{R}\big(RX + (S + \sqrt{\Delta_f}\,)Y\big)\big(RX + (S - \sqrt{\Delta_f}\,)Y\big).$$

Set $U = RX + (S + \sqrt{\Delta_f}\,)Y$ and $V = RX + (S - \sqrt{\Delta_f}\,)Y$ $\Big($so $Q = \frac{1}{2R\sqrt{\Delta_f}}\begin{pmatrix} \sqrt{\Delta_f} - S & \sqrt{\Delta_f} + S \\ R & -R \end{pmatrix}$ and $\epsilon = -1/(2R\sqrt{\Delta_f})\Big)$. Thus, $X = \frac{1}{2R\sqrt{\Delta_f}}\big((\sqrt{\Delta_f} - S)\,U + (\sqrt{\Delta_f} + S)\,V\big)$ and $Y = \frac{1}{2\sqrt{\Delta_f}}(U - V)$. Let $\widetilde{f}(U,V) = f(X(U,V), Y(U,V))$ as above. Because $h_f(U,V) = \frac{36}{R}UV$ we see that $\widetilde{R} = \epsilon^2\overline{R} = 0$ and $\widetilde{T} = \epsilon^2\overline{T} = 0$, showing that $\widetilde{f}$ is diagonal. Indeed $\widetilde{f}(U,V) = a\,U^3 + b\,V^3$, where

$$a \;=\; \widetilde{f}(1,0) \;=\; f\big(\tfrac{\sqrt{\Delta_f} - S}{2R\sqrt{\Delta_f}}, \tfrac{1}{2\sqrt{\Delta_f}}\big) \quad \text{and} \quad b \;=\; \widetilde{f}(0,1) \;=\; f\big(\tfrac{\sqrt{\Delta_f} + S}{2R\sqrt{\Delta_f}}, \tfrac{-1}{2\sqrt{\Delta_f}}\big).$$

The case where $R = 0$ (so $T \neq 0$) is treated analogously by putting $U = (S + \sqrt{\Delta_f}\,)X + TY$ and $V = (S - \sqrt{\Delta_f}\,)X + TY$.

Now, as in earlier sections, for $c \in k^*$ and $\Delta = -c/27$, let $\mathcal{E}$ be the projective elliptic curve with affine model $\mathcal{E}\colon Y^2 = X^3 + c$, and let $\mathcal{T}$ be its subgroup $\{\,\mathcal{O}, (0, \pm\sqrt{c})\,\} \subseteq \mathcal{E}(k_s)$.

Theorem 6.1. *The curves in the image of the canonical map $\Psi\colon H^1(k,\mathcal{T}) \longrightarrow H^1(k,\mathcal{E})$ are all the curves $\mathcal{C}_f$ as in* (6.1) *with $\Delta_f \equiv \Delta \ (mod\ k^{*6})$.*

PROOF. (We thank D. Krashen for suggesting the corestriction argument given at the end of the proof.) Assume first that $\Delta \in k^{*2}$. We saw in the proof of Proposition 2.1 that the curves $\mathcal{C}_t$ in $im(\Psi)$ have the form $\mathcal{C}_t\colon X^3 - tY^3 = -54\,t^2\sqrt{\Delta}\,Z^3$ as t ranges over k^*. This $\mathcal{C}_t$ is the curve $\mathcal{C}_f$ for $f(X,Y) = -\frac{1}{54\,t^2\sqrt{\Delta}}(X^3 - tY^3)$; therefore,

$$\Delta_f \;=\; (-t)^2/[\,4(-54\,t^2\sqrt{\Delta})^4\,] \;=\; \Delta[(18\,t\sqrt{\Delta})^{-6}] \;\equiv\; \Delta \ (mod\ k^{*6}).$$

Now, for any f as in (6.1), suppose that $\Delta_f \equiv \Delta \ (mod\ k^{*6})$. We then have $\Delta_f \in k^{*2}$ by hypothesis. Thus, by changing variables we may diagonalize f, reducing to the case where $B = C = 0$; as we saw above, this change of variables preserves Δ_f modulo k^{*6}. By Corollary 2.2, every $\mathcal{C}_f$ with f diagonal is isomorphic to some $\mathcal{C}_t$. This completes the proof when $\Delta \in k^{*2}$.

Next, assume that $\Delta \notin k^{*2}$. Let $L = k(\sqrt{\Delta})$ and let τ be the nonidentity k-automorphism of L. As we saw in (2.6) above, $H^1(k,\mathcal{T}) \cong \{\,\overline{t} \in L^*/L^{*3} \,\big|\, \tau(\overline{t}) = \overline{t}^{\,-1}\,\}$. Take any $t \in L^*$ with $\tau(t) \equiv t^{-1} \ (mod\ L^{*3})$. Then $t^2/\tau(t)^2 = t\big[t^3/(t\,\tau(t))^2\big] \equiv t \ (mod\ L^{*3})$; so, by replacing t by $t^2/\tau(t)^2$, we may assume that $\tau(t) = t^{-1}$. Let $[\gamma_t] \in H^1(k,T)$ be the cohomology class corresponding to tL^{*3}. Since $\Delta \in L^{*2}$, Proposition 2.1 applies over L and tells us that the curve over L associated to $\Psi_L(res_{k\to L}[\gamma_t])$ is $\mathcal{C}_{t,L}$ with equation

$$\mathcal{C}_{t,L}\colon U^3 - tV^3 \;=\; -54\,t^2\sqrt{\Delta}\,Z^3. \tag{6.4}$$

To see that $\mathcal{C}_{t,L}$ is actually defined over k, we make the change of variables

$$X \;=\; \tfrac{1}{2}(U{+}t^{-1}V) \ \text{ and } \ Y \;=\; \tfrac{\sqrt{\Delta}}{2}(U{-}t^{-1}V), \ \text{ so } \ U \;=\; \tfrac{1}{\sqrt{\Delta}}(\sqrt{\Delta}\,X{+}Y) \ \text{ and } \ V \;=\; \tfrac{t}{\sqrt{\Delta}}(\sqrt{\Delta}\,X{-}Y).$$

Then equation (6.4) becomes

$$-54\,t^2\sqrt{\Delta}\,Z^3 \;=\; U^3 - tV^3 \;=\; \Delta^{-3/2}\big[(\sqrt{\Delta}\,X + Y)^3 - t^4(\sqrt{\Delta}\,X - Y)^3\big],$$

which simplifies to:

$$Z^3 \;=\; AX^3 + 3BX^2Y + 3CXY^2 + DY^3,$$

where

$$A \;=\; \tfrac{t^2-t^{-2}}{54\sqrt{\Delta}}, \quad B \;=\; \tfrac{-(t^2+t^{-2})}{54\Delta}, \quad C \;=\; \tfrac{t^2-t^{-2}}{54\Delta\sqrt{\Delta}}, \quad \text{and} \quad D \;=\; \tfrac{-(t^2+t^{-2})}{54\Delta^2}. \tag{6.5}$$

Since $\tau(\sqrt{\Delta}) = -\sqrt{\Delta}$ and $\tau(t) = t^{-1}$, the constants A, B, C, D are each fixed by τ, so lie in k. Let $g(X,Y) = AX^3 + 3BX^2Y + 3CXY^2 + DY^3$. Then, the curve $\mathcal{C}_g\colon Z^3 = g(X,Y)$ is defined over k, and $\mathcal{C}_g \times_k L \cong \mathcal{C}_{t,L}$ over L. By [An, (3.4), (3.5), (3.8)], the Jacobian of $\mathcal{C}_g$ is the elliptic curve $\mathcal{E}$, which implies that $\mathcal{C}_g$ is the curve determined by some $\theta \in H^1(k,\mathcal{E})$. Hence,

$$res_{k\to L}(\theta) \;=\; \Psi_L(res_{k\to L}[\gamma_t]) \;=\; res_{k\to L}(\Psi[\gamma_t]) \ \text{ in } H^1(L,\mathcal{E}).$$

Arguing as in the proof of Proposition 2.1, since θ has points in a degree 3 field extension of k, it follows that θ is 3-torsion in $H^1(k,\mathcal{E})$. Also $\Psi[\gamma_t]$ is 3-torsion, as $|\mathcal{T}| = 3$. Because $[L\colon k] = 2$, the restriction map $H^1(k,\mathcal{E}) \to H^1(L,\mathcal{E})$ is injective on 3-torsion. Hence, we have $\theta = \Psi[\gamma_t]$, showing

that the curve $\mathcal{C}_g$ lies in $im(\Psi)$. Furthermore, as $(t^2 - t^{-2})^2 - (t^2 + t^{-2})^2 = -4$, for the R, S, T of (6.2) for this g we have

$$R = -(27\Delta)^{-2}, \quad S = 0, \quad \text{and} \quad T = 27^{-2}\Delta^{-3},$$

so $\Delta_g = -RT = (9\Delta)^{-6}\Delta \equiv \Delta \ (mod\ k^{*6})$. Since the choice of $[\gamma_t] \in H^1(k, T)$ was arbitrary, we have shown that every curve in $im(\Psi)$ has the specified form.

Finally, take an arbitrary binary cubic $f(X, Y)$ with $\Delta_f \equiv \Delta \ (mod\ k^{*6})$. It is shown in [An, (3.4), (3.5), (3.8)] that the Jacobian of the curve $\mathcal{C}_f$ is the elliptic curve with affine model $Y^2 = X^3 - 27\Delta_f$, which is isomorphic to the curve $\mathcal{E}\colon Y^2 = X^3 - 27\Delta$ since $\Delta \equiv \Delta_f \ (mod\ k^{*6})$. Thus, $\mathcal{C}_f$ is the curve of some $\varphi \in H^1(k, \mathcal{E})$, and since $\mathcal{C}_f$ has a rational point in some degree 3 extension of k, the restriction-corestriction argument shows t hat $3\varphi = 0$. Let $\varphi_L = res_{k\to L}(\varphi) \in H^1(L, \mathcal{E})$. The earlier case with Δ a square shows that $\varphi_L = \Psi(\delta)$ for some $\delta \in H^1(L, \mathcal{T})$. This δ, which is not uniquely determined, need not lie in $res_{k\to L}(H^1(k, \mathcal{T}))$. But, let $\delta' = 2cor_{L\to k}(\delta) \in H^1(k, \mathcal{T})$. Then, using the compatibility of Ψ with $res_{k\to L}$ and $cor_{L\to k}$, we have

$$\begin{aligned} res_{k\to L}(\Psi(\delta')) &= res_{k\to L}\big(2cor_{L\to k}(\Psi_L(\delta))\big) = res_{k\to L}(2cor_{L\to k}(\varphi_L)) \\ &= res_{k\to L}(2\cdot[L\colon k]\,\varphi) = 4\,res_{k\to L}(\varphi) = res_{k\to L}(\varphi). \end{aligned}$$

Because $2 = [L\colon k]$ is relatively prime to 3, $res_{k\to L}$ is injective on the 3-torsion of $H^1(k, \mathcal{E})$ and therefore $\Psi(\delta') = \varphi$, showing that the curve $\mathcal{C}_f$ lies in $im(\Psi)$. $\square$

Now, take any curve $\mathcal{C}_f$ as in (6.1) with $\Delta_f \notin k^{*2}$, i.e., f is not diagonalizable over k. Set $\Delta = \Delta_f$ and take the elliptic curve $\mathcal{E}\colon Y^2 = X^3 + c$ where $c = -27\Delta$. As in §2 and §3, let $\mathcal{T} = \{\mathcal{O},\ (0, \pm\sqrt{c})\} \subseteq \mathcal{E}(k_s)$, let $\mathcal{E}'$ be the elliptic curve $\mathcal{E}'\colon Y^2 = X^3 + d$ where $d = -27c$ and let $\mathcal{T}' = \{\mathcal{O}',\ (0, \pm\sqrt{d})\} \subseteq \mathcal{E}'(k_s)$, and $\lambda'\colon \mathcal{E}' \to \mathcal{E}$ the isogeny with kernel $\mathcal{T}'$ as in (3.6). By Theorem 6.1, the curve $\mathcal{E}$ is the Jacobian of $\mathcal{C}_f$ and there is $\delta \in H^1(k, \mathcal{T})$ with $\Psi(\delta) \in H^1(k, \mathcal{E})$ corresponding to $\mathcal{C}_f$. Let $\partial\colon \mathcal{E}(k) \to H^1(k, \mathcal{T}')$ be the connecting homomorphism arising from the short exact sequence (3.2). Since $\mathcal{T}' \otimes \mathcal{T} \cong \mu_3$ as G_k-modules, we have the cup product pairing

$$\cup\colon H^1(k, \mathcal{T}') \times H^1(k, \mathcal{T}) \longrightarrow H^2(k, \mu_3) \cong {}_3Br(k),$$

which yields a map

$$\beta\colon \mathcal{E}(k) \to {}_3Br(k) \quad \text{given by} \quad P \mapsto \partial(P) \cup \delta. \tag{6.6}$$

The theorem of Ciperiani and Krashen [CK, Th. 2.6.5] says that $Br(k(\mathcal{C}_f)/k) = im(\beta)$.

As observed earlier in (2.4) and (3.7), we have

$$\mathcal{T} \cong \mathbb{Z}_3(c) \cong \mu_3(\Delta) \ \text{ and } \ \mathcal{T}' \cong \mathbb{Z}_3(\Delta) \cong \mu_3(c) \ \text{ as } G_k\text{-modules}.$$

In the diagonal case considered in earlier sections, when $\Delta \in k^{*2}$, the factors in the cup products $H^1(k, \mathcal{T}') \cup H^1(k, \mathcal{T}) = H^1(k, \mathbb{Z}_3) \cup H^1(k, \mu_3)$ give presentations of the corresponding algebras as cyclic algebras. However, when $\Delta \notin k^{*2}$ and $-3\Delta \notin k^{*2}$, the cup products do not immediately yield cyclic algebra presentations, though we know by Wedderburn's theorem that these degree 3 algebras are cyclic. In this case, to realize the cup products as cyclic algebras one can apply the explicit algorithm given in the proof of [HKRT, Prop. 28] to restate a cup product in $H^1(k, \mu_3(c)) \cup H^1(k, \mu_3(\Delta))$ as a cup product in $H^1(k, \mu_3) \cup H^1(k, \mathbb{Z}_3)$.

The cohomology groups $H^1(k, \mathcal{T})$ and $H^1(k, \mathcal{T}')$ appearing here classify certain cubic field extensions of k, and we want to demonstrate how these field show up in the cup product algebras.

Proposition 6.2. (cf. [HKRT, Prop. 24]) *Let $t \in k^*$. Then the nontrivial cyclic subgroups of $H^1(k, \mathbb{Z}_3(t))$ classify k-isomorphism classes of separable field extensions M of k with $[M:k] = 3$ and $disc(M) \equiv t \ (mod\, k^{*2})$.*

Proof. (This is valid for any field k with $char(k) \neq 2$.) This is standard when $t \in k^{*2}$, so that $\mathbb{Z}_3(t) \cong \mathbb{Z}$ as G_k-modules. In that case for each nonzero $\chi \in H^1(k, \mathbb{Z}_3(t)) \cong Hom(G_k, \mathbb{Z}_3)$ the cyclic group $\langle\chi\rangle$ of order 3 corresponds to the fixed field $k_s^{ker(\chi)}$, which is a cyclic Galois extension of k of degree 3, so of trivial discriminant in k^*/k^{*2}. All of the separable cubic field extensions of k with trivial discriminant arise in this way.

Now, suppose $t \notin k^{*2}$. Let $K = k(\sqrt{t})$ and let σ be the nonidentity k-automorphism of K. The restriction map $H^1(k, \mathbb{Z}_3(t)) \to H^1(K, \mathbb{Z}_3(t)) = H^1(k, \mathbb{Z}_3)$ is injective as $\mathbb{Z}_3(t)$ is 3-torsion and $[K:k] = 2$. We identify $H^1(k, \mathbb{Z}_3(t))$ with its image in $H^1(K, \mathbb{Z}_3)$ which by Proposition 1.1 above consists of those $\chi \in H^1(K, \mathbb{Z}_3)$ with $\sigma(\chi) = \chi^{-1}$. Let N_χ be the fixed field $k_s^{ker(\chi)}$, a cyclic Galois extension of K of degree 3. Recall that $\sigma(\chi)$ is defined as follows: Take any extension σ' of σ to k_s, so $\sigma' \in G_k$. For $\rho \in G_K$, we then have $\sigma(\chi)(\rho) = \chi(\sigma'^{-1}\rho\sigma')$. Since $\sigma(\langle\chi\rangle) = \langle\chi\rangle$, it follows that $ker(\chi)$ is a normal subgroup of G_k; hence N_χ is Galois over k. But the Galois group $\mathcal{G}al(N_\chi/k)$ is nonabelian as $\sigma(\chi) \neq \chi$, so $\mathcal{G}al(N_\chi/k) \cong S_3$, and N_χ contains three different but k-isomorphic subfields M_i with $[M_i:k] = 3$. Since N_χ is the normal closure of each M_i over k, the discriminant of M_i over k is tk^{*2} in k^*/k^{*2}. The correspondence of the proposition is defined by mapping $\langle\chi\rangle$ to the isomorphism class of the M_i. For the inverse of this map, consider a field extension M of k of degree 3 with $disc(M) = tk^{*2}$. Let $N = Mk(\sqrt{t})$, which is the normal closure of M over k; so N is Galois over k with group $\mathcal{G}al(N/k) \cong S_3$. Since N is cyclic Galois over $k(\sqrt{t}) = K$, there is $\eta \in Hom(G_K, \mathbb{Z}_3)$ with $G_N = ker(\eta)$. Because N is Galois over k, $\sigma(\langle\eta\rangle) = \langle\eta\rangle$, but $\sigma(\eta) \neq \eta$ as $\mathcal{G}al(N/k)$ is nonabelian; hence, $\sigma(\eta) = \eta^{-1}$. The map $[M] \mapsto \langle\eta\rangle$ is an inverse of the map of this Proposition, so that map is a bijection. $\square$

Remark 6.3. Suppose $\mu_3 \not\subseteq k$, and take any $u \in k^* \setminus k^{*2}$. Then $H^1(k, \mu_3(u))$ injects into $H^1(k(\sqrt{u}), \mu_3) \cong k(\sqrt{u})^*/k(\sqrt{u})^{*3}$, but also $H^1(k, \mu_3(u)) \cong H^1(k, \mathbb{Z}_3(-3u))$ which we have just seen classifies certain field extensions of k. We can relate these two interpretations of $H^1(k, \mu_3(u))$ as follows: Assume $u \not\equiv -3 \ (mod\, k^{*2})$. Let ρ be the nonidentity k-automorphism of $k(\sqrt{u})$. Take any nonzero $\gamma \in H^1(k, \mu_3(u))$. The injection $H^1(k, \mu_3(u)) \to k(\sqrt{u})/k(\sqrt{u})^{*3}$ maps γ to a cube class $sk(\sqrt{u})^{*3}$ with $s \notin k(\sqrt{u})^{*3}$ such that $\rho(s) \equiv s^{-1} \ (mod\, k(\sqrt{u})^{*3})$, say $\rho(s) = s^{-1}b^3$. Then $\rho(b^3) = b^3$, so $\rho(b) = b$ as $\mu_3 \not\subseteq k(\sqrt{u})$. Choose $r \in k_s$ with $r^3 = s$, and let $F = k(\sqrt{u})(r)$. Since $\mu_3 \not\subseteq k(\sqrt{u})$, there is a unique extension of ρ to an automorphism ρ' of F, determined by $\rho'(r) = r^{-1}b$. Since $\rho'^2(r) = rb^{-1}\rho'(b) = r$, it follows that $\rho'^2 = id_F$. Let M be the fixed field $F^{\rho'}$. Then $[M:k] = 3$, and one can check that M has discriminant $-3uk^{*2}$ in k^*/k^{*2} and that the isomorphism class of M is the one associated to $\gamma \in H^1(k, \mu_3(-3u))$ in Proposition 6.2.

Remark 6.4. The degree 3 algebras A in $Br(k(\mathcal{C}_f)/k)$ with f nondiagonal are realized as cup products of cohomology classes which are associated via Proposition 6.2 to certain cubic field extensions of k. It is interesting to see how those extension fields show up within A. Take $\Delta \in k^* \setminus k^{*2}$ with $-3\Delta \notin k^{*2}$. Take any nonzero $\theta \in H^1(k, \mathbb{Z}_3(\Delta))$ and $\gamma \in H^1(k, \mu_3(\Delta))$, and let A be the degree 3 central simple k-algebra corresponding to $\theta \cup \gamma$ in ${}_3Br(k)$. Let $L = k(\sqrt{\Delta})$ and let τ be the nonidentity k-automorphism of L. Let $A_L = A \otimes_k L$ and let $\theta_L = res_{k\to L}(\theta) \in H^1(L, \mathbb{Z}_3) = Hom(G_L, \mathbb{Z}_3)$, and $\gamma_L = res_{k\to L}(\gamma) \in H^1(L, \mu_3) \cong L^*/L^{*3}$. Since $A_L = \theta_L \cup \gamma_L \in {}_3Br(L)$, we can write $A_L = (N/L, \sigma, t)$ where $N = k_s^{ker(\theta_L)}$, which is the cyclic Galois extension of L of degree 3 associated with θ_L, and $tL^{*3} \in L^*/L^{*3}$ corresponds to γ_L. Because $\theta_L \in im\big(res_{k\to L}H^1(k, \mathbb{Z}_3(\Delta))\big)$, by Proposition 1.1, $\tau(\theta_L) = \theta_L^{-1}$. Consequently, N is Galois but not abelian Galois over k, so $\mathcal{G}al(N/k) \cong S_3$. The automorphism τ of L extends to an automorphism $\overline{\tau}$ of N of order 2. (There

are three different possibilities for $\overline{\tau}$; choose any one of them.) Then the fixed field $M = N^{\overline{\tau}}$ is a cubic extension of k in the isomorphism class associated to θ in Proposition 6.2. Note also that $\overline{\tau}\sigma\overline{\tau}^{-1} = \sigma^{-1}$ as $\mathcal{G}al(N/k) \cong S_3$. Now, $A_L = \bigoplus_{i=0}^{2} Nx^i$ where $xrx^{-1} = \sigma(r)$ for all $r \in N$ and $x^3 = t$. Because $\gamma_L \in im\big(res_{k\to L}(H^1(k, \mu_3(\Delta))\big)$, we have $\tau(t) = t^{-1}b^3$ for some $b \in L^*$. Then $\tau(b^3) = b^3$ and hence $\tau(b) = b$ as $\mu_3 \not\subseteq L$. Extend $\overline{\tau}$ on N to a map $\widetilde{\tau}\colon A_L \to A_L$ by sending $x \mapsto x^{-1}b$, i.e., $\widetilde{\tau}(\sum_{i=0}^{2} r_i x^i) = \sum_{i=0}^{2} \overline{\tau}(r_i)(x^{-1}b)^i$. Clearly, $\widetilde{\tau}$ is bijective. Because $\widetilde{\tau}$ respects the relations defining A_L it is a ring isomorphism, which restricts to τ on L. Also, as $\overline{\tau}^2 = id_N$ and $\widetilde{\tau}^2(x) = xb^{-1}\tau(b) = x$, we have $\widetilde{\tau}^2 = id$. Thus, $\widetilde{\tau}$ yields a semilinear action of $\mathcal{G}al(L/k)$ on A_L. Consequently, if we let $B = A_L^{\widetilde{\tau}}$, the fixed ring of A_L under the action of $\widetilde{\tau}$, then B is a k-algebra with $B \otimes_k L \cong A_L$ (L-algebra isomorphism) (cf. [J, p. 56, Lemma 2.13.1]). Therefore, B is a central simple k-algebra. Since $res\colon {}_3Br(k) \to {}_3Br(L)$ is injective as $[L\colon k] = 2$, it follows that $B \cong A$. Notice that B contains $N^{\widetilde{\tau}} = N^{\overline{\tau}} = M$, the field corresponding to θ. But, $\widetilde{\tau}$ also maps $k(x)$ to itself and, as noted in Remark 6.3, the fixed field $k(x)^{\widetilde{\tau}}$ is the degree 3 field extension of k with discriminant $-3\Delta k^{*2} \in k^*/k^{*2}$ which corresponds to γ viewed in $H^1(k, \mathbb{Z}_3(-3\Delta))$. Thus, as $A \cong B$, A contains copies of the field M corresponding to θ and the field $F(x)^{\widetilde{\tau}}$ corresponding to γ, in such a way that $M \otimes_k L$ and $F(x)^{\widetilde{\tau}} \otimes_k L$ are the usual subfields in $A \otimes_k L$ viewed as $\theta_L \cup \gamma_L$.

We now give a few specific examples of relative Brauer groups of function fields of nondiagonal cubic forms over $\mathbb{Q}$.

Example 6.5. Consider $\mathcal{C}_f\colon Z^3 = f(X,Y)$ where

$$f(X,Y) = 13X^3 + 3{\cdot}7X^2Y + 3{\cdot}19XY^2 - 5Y^3.$$

The discriminant of f is $88209 = 297^2 \in \mathbb{Q}^{*2}$, so f is diagonalizable. Put $X = \frac{1}{3}(U + 2V)$ and $Y = \frac{1}{3}(-U + V)$, which gives $\widetilde{f}(U,V) = 2U^3 + 11V^3$. Since $\mathcal{C}_f \cong \mathcal{C}_{\widetilde{f}}$, from Example 5.13 we have

$$Br(\mathbb{Q}(\mathcal{C}_f)/\mathbb{Q}) = Br(k(\mathcal{C}_f)/k) = \{\,0\,\},$$

where $k = \mathbb{Q}(\omega)$.

Example 6.6. Consider $\mathcal{C}_f\colon Z^3 = f(X,Y)$ where

$$f(X,Y) = 4X^3 + 3{\cdot}4XY^2 + 4Y^3.$$

The discriminant Δ of f is $320 = 2^6{\cdot}5 \notin \mathbb{Q}^{*2}$, so f is not diagonalizable over $\mathbb{Q}$ but is diagonalizable over $\mathbb{Q}(\sqrt{5}\,)$. The Jacobian of $\mathcal{C}$ is $Y^2 = X^3 - 27\Delta = X^3 - 27{\cdot}2^6{\cdot}5$. Thus, we can use the isomorphic elliptic curve $\mathcal{E}\colon Y^2 = X^3 - 27{\cdot}5$, so $c = -27{\cdot}5$, and the isogenous curve $\mathcal{E}'\colon Y^2 = X^3 + 5$. By SAGE, it is known that $\mathcal{E}(\mathbb{Q})$ has rank 1 with generator $(6,9)$ and that $\mathcal{E}'(\mathbb{Q})$ has generator $(-1,2)$. Note that $\alpha(6,9) = \overline{9+\sqrt{c}} = \overline{9 + 3\sqrt{-15}}$ in $\mathbb{Q}(\sqrt{-15})^*/\mathbb{Q}(\sqrt{-15})^{*3}$ and $\alpha'(1,2) = \overline{2+\sqrt{5}} = \overline{1}$ in $\mathbb{Q}(\sqrt{5})^*/\mathbb{Q}(\sqrt{5})^{*3}$, as $2+\sqrt{5} = \big((1+\sqrt{5})/2\big)^3$. According to (5.7), we see that $\mathcal{E}(\mathbb{Q})$ and $\mathcal{E}'(\mathbb{Q})$ are torsion-free. Thus, it follows from (5.4) that

$$\alpha(\mathcal{E}(\mathbb{Q})) = \big\langle\, \overline{9 + 3\sqrt{-3{\cdot}5}}\,\big\rangle \subseteq \mathbb{Q}(\sqrt{-15})^*/\mathbb{Q}(\sqrt{-15})^{*3} \quad\text{and}\quad \alpha'(\mathcal{E}'(\mathbb{Q})) = \langle\,\overline{1}\,\rangle.$$

Because the map $\mathcal{E}(\mathbb{Q}) \to Br(\mathbb{Q}(\mathcal{C}_f)/\mathbb{Q})$ is surjective, the relative Brauer group $Br(\mathbb{Q}(\mathcal{C}_f)/\mathbb{Q})$ is completely determined by what this map does to the generator $(6,9)$.

Let $k = \mathbb{Q}(\sqrt{5})$ and $L = \mathbb{Q}(\sqrt{5}, \omega)$. We have the following commutative diagram:

$$\begin{array}{ccccc}
\mathcal{E}(L) & \longrightarrow & Br(L(\mathcal{C}_f)/L) & = & Br(L(\mathcal{C}_{\widetilde{f}})/L) \\
\uparrow & & \uparrow & & \uparrow \\
\mathcal{E}(k) & \longrightarrow & Br(k(\mathcal{C}_f)/k) & = & Br(k(\mathcal{C}_{\widetilde{f}})/k) \\
\uparrow & & \uparrow & & \\
\mathcal{E}(\mathbb{Q}) & \longrightarrow & Br(\mathbb{Q}(\mathcal{C}_f)/\mathbb{Q}) & &
\end{array}$$

Here all the vertical maps are injective and the horizontal maps are surjective. We know f is diagonalizable over k. Specifically, put $X = \frac{1}{2}(1+\sqrt{5})U + \frac{1}{2}(1-\sqrt{5})V$ and $Y = -U - V$; then, $\widetilde{f}(U, V) = \widetilde{a}\,U^3 + \widetilde{b}\,V^3$, where

$$\widetilde{a} \,=\, f\big(\tfrac{1}{2}(1+\sqrt{5}), -1\big) \,=\, 10(1+\sqrt{5}) \quad \text{and} \quad \widetilde{b} \,=\, f\big(\tfrac{1}{2}(1-\sqrt{5}), -1\big) \,=\, 10(1-\sqrt{5}).$$

We have $\mathcal{C}_f \cong \mathcal{C}_{\widetilde{f}}$ over k and the Jacobian is up to isomorphism $\mathcal{E}\colon Y^2 = X^3 - 27{\cdot}\sqrt{5}^{\,2}$. Thus, by Remark 4.2(ii) the image of $(6, 9) \in \mathcal{E}(k)$ in $Br(L(\mathcal{C}_{\widetilde{f}})/L)$ is the Brauer class of the symbol algebra

$$A := \,(t, u)_\omega,$$

where $t = -\widetilde{b}/\widetilde{a} = -(1-\sqrt{5})/(1+\sqrt{5}) = (3-\sqrt{5})/2$ and $u = 3(3+\sqrt{-15})$. For this t the nonidentity automorphism of $\mathbb{Q}(\sqrt{5})$ maps t to t^{-1}. Hence $(t) \in H^1(\mathbb{Q}, \mathcal{T}) = H^1(\mathbb{Q}, \mu_3(5)) \subseteq \mathbb{Q}(\sqrt{5})^*/\mathbb{Q}(\sqrt{5})^{*3}$. Likewise, the nonidentity automorphism of $\mathbb{Q}(\sqrt{-15})$ maps u to $3(3-\sqrt{-15}) = 6^3u^{-1}$, so $(u) \in H^1(\mathbb{Q}, \mathcal{T}') = H^1(\mathbb{Q}, \mu_3(-15)) \subseteq \mathbb{Q}(\sqrt{-15})^*/\mathbb{Q}(\sqrt{-15})^{*3}$. The algebra we seek is the cup product $(u) \cup (t)$ in $H^2(\mathbb{Q}, \mu_3) \cong {}_3Br(\mathbb{Q})$, which maps to A in ${}_3Br(L)$. We will describe this algebra and its inverse by their local invariants. Observe that each nonidentity $\sigma \in \mathcal{G}al(L/\mathbb{Q})$ maps exactly two of t, u, ω to their inverses in L^*/L^{*3} while fixing the third element; hence, σ maps $[A]$ to $[A]$ in $Br(L)$. Therefore, the local invariants for $[A]$ are the same at each prime of L over a given prime of $\mathbb{Q}$. This assures that A is defined over $\mathbb{Q}$, as expected.

We now check that the symbol algebra A above is nonsplit over L by looking at a 2-adic completion. For the 2-adic completion $\widehat{\mathbb{Q}}_2$, note that $\widehat{\mathbb{Q}}_2(\sqrt{5})$ and $\widehat{\mathbb{Q}}_2(\sqrt{-3})$ are each the unramified quadratic extension of $\widehat{\mathbb{Q}}_2$. On the other hand, the 2-adic valuation on $\mathbb{Q}$ splits over $\mathbb{Q}(\sqrt{-15})$ so it splits over L; let $\widehat{L}_2$ be the completion of L with respect to either of it 2-adic valuations. Then $\widehat{L}_2$ is the unramified quadratic extension of $\widehat{\mathbb{Q}}_2$. Let $v\colon \widehat{L}_2^* \to \mathbb{Z}$ denote the corresponding discrete valuation. Since the ramification of $A \otimes_L \widehat{L}_2$ in $H^1(\overline{L}_2, \mathbb{Z}_3) \cong \overline{L}_2^*/\overline{L}_2^{*3}$ is the residue of $(-1)^{v(t)v(u)}t^{v(u)}u^{-v(t)}$, we will verify that

$$v(t) = 0, \;\; \overline{t} \notin \overline{L}_2^{*3}, \;\text{ and }\; v(u) = 1 \text{ or } 2 \;\text{ depending on the choice of } v. \tag{6.7}$$

Hence, $A \otimes_L \widehat{L}_2$ has nontrivial ramification, so is nonsplit;, hence, A is nonsplit.

To verify (6.7), first observe that $t = -\frac{1-\sqrt{5}}{2} \cdot \frac{2}{1+\sqrt{5}}$ is a 2-adic unit. Since the minimal polynomial of t over $\mathbb{Q}$ is $X^2 - 3X + 1$, it follows that $\overline{t}$ is a root of $X^2 + X + 1$ over $\overline{L}_2 \cong \mathbb{F}_4$. Hence, $\overline{t} \neq \overline{1}$ in $\overline{L}_2^*$, so $\overline{t} \notin \overline{L}_2^{*3}$. In order to show that $v(u) = v(3+\sqrt{-15}) = 1$ or 2, let $a = \sqrt{-15}$ over $\widehat{L}_2$. Since $(a+1)(a-1) = -16$ and $a+1 = (a-1)+2$, the only possibilities are $v(a+1) = 1$

and $v(a-1)=3$, or vice versa. When $v(a-1)=3$, we have $v(3+\sqrt{-15})=v(4+(a-1))=2$. On the other hand, when $v(a+1)=3$, we have $v(3+\sqrt{-15})=v(2+(a+1))=1$, as claimed in (6.7).

Now, notice that the only other prime where A is potentially nonsplit is the unique 3-adic prime of L since t and u are valuation units for all prime spots above $p \neq 2,3$ over $\mathbb{Q}$. Since the sum of the local invariants is 0 in $\mathbb{Q}/\mathbb{Z}$, the algebra B corresponding to $(u)\cup(t)$ over $\mathbb{Q}$ has either local invariant $\frac{1}{3}$ at 2, hence $\frac{2}{3}$ at 3, and 0 everywhere else; or $\frac{2}{3}$ at 2, hence $\frac{1}{3}$ at 3, and 0 everywhere else. The second possibility corresponds to the inverse of the first in $Br(\mathbb{Q})$. Which possibility occurs depends on the choices of $\sqrt{-3}$, $\sqrt{5}$, and $\sqrt{-15}$. In either case,

$$Br(\mathbb{Q}(\mathcal{C}_f)/\mathbb{Q}) \;=\; \big\langle\, [(u)\cup(t)] \,\big\rangle \;\cong\; \mathbb{Z}/3\mathbb{Z},$$

and the two algebras over $\mathbb{Q}$ we have specified by local invariants are the two nonidentity elements of this group.

§7. The generalized Clifford algebra of f

As mentioned in the Introduction and in the proof of Proposition 4.1, $Br(k(\mathcal{C}_f)/k)$ consists of the specializations of the generalized Clifford algebra $A_{f,k}$ associated to a binary cubic form f over k; when Δ_f and -3 are squares in k, a presentation of the quotient ring of $A_{f,k}$ as a symbol algebra yields immediately a description of the algebras of degree 3 in $Br(k(\mathcal{C}_f)/k)$ as symbol algebras. We now relate the results of the preceding sections to the structure of the Clifford algebra and its ring of central quotients $q(A_{f,k})$. We denote $q(A_{f,k})$ by $Q_{f,k}$. We will give an explicit description of $Q_{f,k}$ as

(1) a symbol algebra if f is diagonal and $-3 \in k^{*2}$;
(2) a cyclic algebra if f is diagonal and $-3 \notin k^{*2}$;
(3) a cup product in $H^1(Z,\mathcal{T}) \cup H^1(Z,\mathcal{T}')$ if f is not diagonalizable over k,

where $Z = Z(Q_{f,k}) \cong k(\mathcal{E})$. We will further show that $Q_{f,k}$ contains a maximal subfield isomorphic to $k(\mathcal{E}')$. We will also show how $Q_{f,k}$ is related to the curve $\mathcal{C}_f$ in the Brauer group $Br(\mathcal{E})$ of the elliptic curve $\mathcal{E}$ which is the Jacobian of $\mathcal{C}_f$.

We work first with f diagonal over a base field L, which can be any infinite field with $char(L) \neq 2,3$. Let $f(X,Y) = aX^3 + bY^3 \in L[X,Y]$, for some $a,b \in L^*$. Let $A_{f,L}$ be the generalized Clifford algebra of f over L. Thus,

$$A_{f,L} = L\{x,y\} \text{ with defining relations } (px+qy)^3 = f(p,q) \text{ for all } p,q \in L^*.$$

It is known (see[H_1]) that $A_{f,L}$ is an Azumaya algebra over its center $Z = Z(A_{f,L})$ which is an integral domain. Let $q(Z)$ be the quotient field of Z, and let $Q_{f,L} = q(A_{f,L}) \cong A_{f,L} \otimes_Z q(Z)$. It is easy to see that the defining relations for $A_{f,L}$ are equivalent to the basic relations

$$x^3 = a, \quad x^2y + xyx + yx^2 = 0, \quad xy^2 + yxy + y^2x = 0, \quad y^3 = b. \tag{7.1}$$

Let $\Delta_f = a^2b^2/4$, the discriminant of f, and let $c = -27a^2b^2/4 = -27\Delta_f$. Thus, for the projective curve $\mathcal{C}_f\colon Z^3 = f(X,Y)$, the Jacobian of $\mathcal{C}_f$ is the projective elliptic curve $\mathcal{E}\colon Y^2 = Z^3 + c$. (As usual, we are describing projective elliptic curves in terms of their affine models.)

Let $F = L(\omega)$, where ω is a fixed primitive cube root of unity (possibly $F = L$). For the Clifford algebra $A_{f,F}$ of f over F, we have $A_{f,F} \cong A_{f,L} \otimes_L F$. We recall the description of $A_{f,F}$ given in [H_1]: Let

$$z = yx - \omega xy \quad \text{and} \quad \overline{z} = yx - \omega^2 xy.$$

The following identities follow easily from the basic identities (7.1) (see [H_1, Lemma 1.5]):

$$xz = \omega zx, \quad yz = \omega^2 zy, \quad x\overline{z} = \omega^2 \overline{z}x, \quad y\overline{z} = \omega\overline{z}y, \quad z\overline{z} = \overline{z}z. \tag{7.2}$$

One more useful fact is that

$$(yx^{-1})^3 = b/a. \tag{7.3}$$

This is not transparent since x and y don't commute; here is a proof using the basic identities (7.1):

$$\begin{aligned}(yx^{-1})^3 &= a^{-3}y(x^2y)(x^2yx^2) = -a^{-3}y(xyx+yx^2)x^2yx^2 = -a^{-2}(yxy+y^2x)yx^2 \\ &= a^{-2}xy^2yx^2 = b/a\end{aligned}$$

To fix a choice of $\sqrt{c}$, set $\sqrt{c} = \frac{3}{2}(\omega - \omega^2)ab = \frac{3}{2}(2\omega+1)ab$. Let

$$\mathfrak{r} = z\overline{z} \quad \text{and} \quad \mathfrak{s} = \tfrac{1}{2}(z^3 + \overline{z}^3).$$

It follows from the identities in (7.2) that $z\overline{z}$, z^3, $\overline{z}^3$ commute with x and y; hence $\mathfrak{r}$ and $\mathfrak{s}$ lie in the center $Z(A_{f,F})$.

Lemma 7.1. *$z^3 = \mathfrak{s} + \sqrt{c}$ and $\overline{z}^3 = \mathfrak{s} - \sqrt{c}$. Hence, $\mathfrak{r}^3 = \mathfrak{s}^2 - c$.*

Proof. These essential formulas were proved in [H_1, p. 1274] using a matrix representation of $A_{f,F}$. For the convenience of the reader, we now give a proof directly from the identities in (7.1) and (7.2). Let $\alpha = yx$ and $\beta = xy$, so $z = \alpha - \omega\beta$ and $\overline{z} = \alpha - \omega^2\beta$. Also, using (7.1), we have

$$\alpha\beta \;=\; -y(xyx + yx^2) \;=\; -(yxy + y^2x)x \;=\; \beta\alpha.$$

Hence,

$$\begin{aligned}\mathfrak{r} \;&=\; z\overline{z} \;=\; (\alpha - \omega\beta)(\alpha - \omega^2\beta) \;=\; \alpha^2 + \alpha\beta + \beta^2\\ &=\; (yxy)x + xy^2x + \beta^2 \;=\; \beta^2 - y^2x^2;\end{aligned}$$

likewise, $\mathfrak{r} = \alpha^2 - x^2y^2$. Hence,

$$\beta^3 \;=\; (\mathfrak{r} + y^2x^2)\beta \;=\; \mathfrak{r}\beta + y^2x^3y \;=\; \mathfrak{r}\beta + ab, \quad \text{and likewise} \quad \alpha^3 \;=\; \mathfrak{r}\alpha + ab.$$

Thus,

$$\begin{aligned}2ab \;&=\; (\alpha^3 - \mathfrak{r}\alpha) + (\beta^3 - \mathfrak{r}\beta) \;=\; (\alpha^3 + \beta^3) - \mathfrak{r}(\alpha + \beta)\\ &=\; (\alpha^2 - \alpha\beta + \beta^2 - \mathfrak{r})(\alpha + \beta) \;=\; -2\alpha\beta(\alpha + \beta).\end{aligned}$$

This yields

$$\begin{aligned}z^3 - \overline{z}^3 \;&=\; (\alpha - \omega\beta)^3 - (\alpha - \omega^2\beta)^3 \;=\; (-3\omega + 3\omega^2)\alpha^2\beta + (3\omega^2 - 3\omega)\alpha\beta^2\\ &=\; (3\omega^2 - 3\omega)\alpha\beta(\alpha + \beta) \;=\; -(3\omega^2 - 3\omega)ab \;=\; 2\sqrt{c}.\end{aligned}$$

Since $z^3 + \overline{z}^3 = 2\mathfrak{s}$ by definition, we thus have $z^3 = \mathfrak{s} + \sqrt{c}$, $\overline{z}^3 = \mathfrak{s} - \sqrt{c}$, and $\mathfrak{r}^3 = z^3\overline{z}^3 = \mathfrak{s}^2 - c$. $\square$

It was shown in [H_1, Th. 1.1] that $A_{f,F}$ is an Azumaya algebra of rank 9 over its center $Z(A_{f,F})$, and that $Z(A_{f,F}) = F[\mathfrak{r}, \mathfrak{s}]$, and this ring is isomorphic to the coordinate ring over F of an affine piece of $\mathcal{E}$. Thus, for the quotient field we have $q(Z(A_{f,F})) = F(\mathfrak{r}, \mathfrak{s}) \cong F(\mathcal{E})$.

Proposition 7.2. *With notation as above, for $f = aX^3 + bY^3$, the ring of quotients $Q_{f,F}$ of the Clifford algebra $A_{f,F}$ is a symbol algebra,*

$$Q_{f,F} \;=\; F(\mathfrak{r}, \mathfrak{s})\{x, z\} \;\cong\; \big(a,\, \mathfrak{s} + \sqrt{c}; F(\mathfrak{r}, \mathfrak{s})\big)_\omega \;\cong\; \big(b/a,\, \mathfrak{s} + \sqrt{c}; F(\mathfrak{r}, \mathfrak{s})\big)_\omega\,,$$

and $Q_{f,L}$ is a cyclic algebra,

$$Q_{f,L} \;=\; \big(L(\mathfrak{r}, \mathfrak{s})(u)/L(\mathfrak{r}, \mathfrak{s}),\, \rho,\, a\big) \;\cong\; \big(L(\mathfrak{r}, \mathfrak{s})(u)/L(\mathfrak{r}, \mathfrak{s}),\, \rho,\, b/a\big),$$

where $u = z + \overline{z}$, which has minimal polynomial $X^3 - \mathfrak{r}X - 2\mathfrak{s}$ over $L(\mathfrak{r}, \mathfrak{s})$.

Proof. The formulas for $Q_{f,F}$ except the last were given in [H_1], and follow easily from the facts noted above. Specifically, since $x^3 = a$, $z^3 = \mathfrak{s} + \sqrt{c}$, and $xz = \omega zx$, it follows that $F(\mathfrak{r}, \mathfrak{s})\{x, z\} \cong \big(a,\, \mathfrak{s} + \sqrt{c}; F(\mathfrak{r}, \mathfrak{s})\big)_\omega$, which by dimension count is all of $Q_{f,F}$. Likewise, by (7.3) and (7.2) we have $(yx^{-1})^3 = b/a$ and $(yx^{-1})z = \omega z(yx^{-1})$, so $Q_{f,F} \cong \big(b/a,\, \mathfrak{s} + \sqrt{c}; F(\mathfrak{r}, \mathfrak{s})\big)_\omega$.

Let $K = F(\mathfrak{r},\mathfrak{s})(z)$, which is a maximal subfield of $Q_{f,F}$ and is a cyclic Galois extension of $F(\mathfrak{r},\mathfrak{s})$ as $\omega \in F(\mathfrak{r},\mathfrak{s})$ and $z^3 \in F(\mathfrak{r},\mathfrak{s})$ but $z \notin F(\mathfrak{r},\mathfrak{s})$ as z is not central in $A_{f,F}$. Let ρ be the $F(\mathfrak{r},\mathfrak{s})$-automorphism of K with $\rho(z) = \omega z$. Then, $\rho(\overline{z}) = \rho(rz^{-1}) = \omega^2\overline{z}$. Thus, for $u = z + \overline{z} \in K \setminus F(\mathfrak{r},\mathfrak{s})$, we have $K = F(\mathfrak{r},\mathfrak{s})(u)$ since $[K\colon F(\mathfrak{r},\mathfrak{s})] = 3$. Also, we have $\rho(u) = \omega z + \omega^2\overline{z} = xux^{-1} = (yx^{-1})u(yx^{-1})^{-1}$. Hence, conjugation by x or yx^{-1} induces ρ on K, showing that

$$Q_{f,F} \cong \big(F(\mathfrak{r},\mathfrak{s})(u)/F(\mathfrak{r},\mathfrak{s}),\, \rho,\, a\big) \cong \big(F(\mathfrak{r},\mathfrak{s})(u)/F(\mathfrak{r},\mathfrak{s}),\, \rho,\, b/a\big).$$

By expanding out $u^3 = (z+\overline{z})^3$ using $z\overline{z} = \mathfrak{r}$ and $z^3 + \overline{z}^3 = 2s$, we find that $u^3 - \mathfrak{r}u - 2\mathfrak{s} = 0$; this determines the minimal polynomial of u over $F(\mathfrak{r},\mathfrak{s})$. This completes the proof if $L = F$.

Suppose now that $L \neq F$. We argue by descent from F to L. Let σ be the nonidentity L-isomorphism of $F = L(\omega)$. Let σ also denote the canonical extension $id_{Q_{f,L}} \otimes \sigma$ of σ to $Q_{f,F} = Q_{f,L} \otimes_L F$. Since $A_{f,F} = A_{f,L} \otimes_L F$, we have $A_{f,L}$ is the fixed ring ${A_{f,F}}^{\sigma}$ and $Q_{f,L} = {Q_{f,F}}^{\sigma}$. Furthermore, $\sigma(\omega) = \omega^2$, $\sigma(x) = x$, and $\sigma(y) = y$, so $\sigma(z) = \overline{z}$, $\sigma(\overline{z}) = z$, $\sigma(\mathfrak{r}) = \mathfrak{r}$, and $\sigma(\mathfrak{s}) = \mathfrak{s}$. We thus obtain $Z(A_{f,L}) = (Z(A_{f,F}))^{\sigma} = F[\mathfrak{r},\mathfrak{s}]^{\sigma} = L[\mathfrak{r},\mathfrak{s}]$. Since $\sigma(u) = u$, we have $\sigma(K) = K$ and $K^{\sigma} = F(\mathfrak{r},\mathfrak{s})(u)^{\sigma} = L(\mathfrak{r},\mathfrak{s})(u)$, with $[K^{\sigma}\colon L(\mathfrak{r},\mathfrak{s})] = [K\colon F(\mathfrak{r},\mathfrak{s})] = 3$; so K^{σ} is a maximal subfield of $Q_{f,L}$. Also, $\sigma\rho(u) = \omega z + \omega^2\overline{z} = \rho(u)$, so $\rho(K^{\sigma}) = K^{\sigma}$ and $\rho|_{K^{\sigma}}$ is an automorphism (of order 3) of K^{σ}. Hence, K^{σ} is a cyclic Galois extension of $F(\mathfrak{r},\mathfrak{s})^{\sigma} = L(\mathfrak{r},\mathfrak{s})$, with $\rho|_{K^{\sigma}}$ a generator of the Galois group. Conjugation by x (or by yx^{-1}) induces ρ on K and hence on K^{σ}, and $x, yx^{-1} \in Q_{f,L}$ with x^3 and $(yx^{-1})^3$ central. This yields the desired descriptions of $Q_{f,L}$ as a cyclic algebra. The minimal polynomial of u over $F(\mathfrak{r},\mathfrak{s})$ has coefficients in $L(\mathfrak{r},\mathfrak{s})$, so it is also the minimal polynomial of u over $L(\mathfrak{r},\mathfrak{s})$. $\square$

From the description of $Q_{f,L}$ and $Q_{f,F}$ as cyclic and symbol algebras, one can see immediately that their specializations at the points of $\mathcal{E}(L)$ and $\mathcal{E}(F)$ coincide with $Br(L(\mathcal{C}_f)/L)$ and $Br(F(\mathcal{C}_f)/F)$ as given in Propositions 4.1 and 4.4 above.

Now let $d = -27c$ and let $\mathcal{E}'$ be the projective elliptic curve $\mathcal{E}'\colon Y^2 = X^3 + d$. It is clear from Cor. 4.6 and the exact sequence $\mathcal{E}'(k) \xrightarrow{\lambda'} \mathcal{E}(k) \xrightarrow{\partial} H^1(k, \mathcal{T}')$ that the points in $\mathcal{E}(k)$ in the image of $\mathcal{E}'(k)$ under λ' have trivial image in $Br(k(\mathcal{C}_f)/k)$; so at these points the specializations of $Q_{f,k}$ must be split algebras. The next two propositions show how to see this from the structure of $Q_{f,k}$. We first show this in the diagonal case with ground field L and $f(X,Y) = aX^3 + bY^3$. We retain the notation used in Proposition 7.2 and its proof. In particular we let $K = F(\mathfrak{r},\mathfrak{s})(u)$, a maximal subfield of $Q_{f,F}$.

Proposition 7.3. *For the maximal subfield $K = F(\mathfrak{r},\mathfrak{s})(u)$ of $Q_{f,F}$ as above, we have $K \cong F(\mathcal{E}')$. If $\omega \notin L$, so $F = L(\omega) \supsetneqq L$, then K^{σ} is a maximal subfield of $Q_{f,L}$, isomorphic to $L(\mathcal{E}')$.*

Proof. Let $\mathfrak{r}' = 6\sqrt{c}/(z-\overline{z})$ and $\mathfrak{s}' = 9\sqrt{c}\,(z+\overline{z})/(z-\overline{z})$, both lying in $K = F(\mathfrak{r},\mathfrak{s})(z)$. Since $z^3 = \mathfrak{s} + \sqrt{c}$ and $\overline{z} = \mathfrak{r}z^{-1}$ with $\mathfrak{s}^2 = \mathfrak{r}^3 + c$, the proof of Lemma 3.1 (with $\mathfrak{r}$, $\mathfrak{s}$, z, $\overline{z}$ replacing x, y, t, $\widehat{t}$) shows that $\mathfrak{s}'^2 = \mathfrak{r}'^3 + d$, $\mathfrak{r} = (\mathfrak{r}'^3 + 4d)/9\mathfrak{r}'^2$ and $\mathfrak{s} = (\mathfrak{s}'^3 - 9d\mathfrak{s}')/27\mathfrak{r}'^3$. Also, $z + \overline{z} = 2\mathfrak{s}'/3\mathfrak{r}'$. Thus,

$$K = F(\mathfrak{r},\mathfrak{s})(z) = F(\mathfrak{r},\mathfrak{s})(z+\overline{z}) = F(\mathfrak{r},\mathfrak{s},z+\overline{z},\mathfrak{r}',\mathfrak{s}') = F(\mathfrak{r}',\mathfrak{s}').$$

Since K has transcendence degree 1 over F, $F(\mathfrak{r}',\mathfrak{s}') \cong F(\mathcal{E}')$.

Now, assume that $L \neq F$, and let σ be as in the proof of Proposition 7.2. Since $\sigma(z) = \overline{z}$ and $\sigma(\sqrt{c}) = -\sqrt{c}$ (as $\sqrt{c} = \frac{3}{2}(\omega - \omega^2)ab$), we have $\sigma(\mathfrak{r}') = \mathfrak{r}'$ and $\sigma(\mathfrak{s}') = \mathfrak{s}'$. Hence, $K^{\sigma} = F(\mathfrak{r}',\mathfrak{s}')^{\sigma} = L(\mathfrak{r}',\mathfrak{s}')$, and $L(\mathfrak{r}',\mathfrak{s}') \cong L(\mathcal{E}')$ for the same reason that $F(\mathfrak{r}',\mathfrak{s}') \cong F(\mathcal{E}')$. $\square$

Note that the proof of Proposition 7.3 shows that the map on function fields $L(\mathcal{E}) \to L(\mathcal{E}')$ arising from the isogeny $\lambda' \colon \mathcal{E}' \to \mathcal{E}$ given in (3.6) coincides with the inclusion $L(\mathfrak{r},\mathfrak{s}) \to K^\sigma$. Whenever a point $(r,s) \in \mathcal{E}(L)$ equals $\lambda'(r',s')$ for some $(r',s') \in \mathcal{E}'(L)$, then

$$\lambda'^{-1}(r,s) \;=\; \{(r',s'),\,(r',s')\oplus(0,\sqrt{d}),\,(r',s')\oplus(0,-\sqrt{d})\} \;\subseteq \mathcal{E}'(L).$$

The specialization of K^σ at (r,s) is the direct sum of the field extensions of L determined by the points in $\lambda'^{-1}(r,s)$, which here is $L \oplus L \oplus L$. Thus, the specialization of $Q_{f,L}$ at (r,s) must split since it contains the specialization of K^σ.

We now prove analogues to Propositions 7.2 and 7.3 when the form is not diagonalizable over the ground field. This will be done by descent from the quadratic extension over which the form is diagonalizable. For this, let k be the ground field ($char(k) \neq 2,3$), and let

$$\widehat{f}(X,Y) \;=\; AX^3 + 3BX^2Y + 3CXY^2 + DY^3 \in k[X,Y]. \tag{7.4}$$

As in (6.2), let $R = AC - B^2$, $2S = AD - BC$, $T = BD - C^2$, and $\Delta_{\widehat{f}} = S^2 - RT$, which is assumed nonzero. We assume $\widehat{f}$ is not diagonalizable over k, so $\Delta_{\widehat{f}} \notin k^{*2}$, which implies that $RT \neq 0$. Let δ be a fixed square root of $\Delta_{\widehat{f}}$ and let $L = k(\delta)$. Let $f(X,Y) = aX^3 + bY^3$ be the diagonalization of $\widehat{f}$ over L that was constructed in §6.

To carry out the descent from L to k, we must see how $Q_{\widehat{f},k}$ sits within $Q_{f,L}$. For this, recall the change of variables used in §6. Matrix notation is convenient. We write $f\binom{X}{Y}$ for $f(X,Y)$, likewise for $\widehat{f}$. As in §6, set $U = RX + (S+\delta)Y$ and $V = RX + (S-\delta)Y$, i.e., $\binom{U}{V} = P\binom{X}{Y}$ where $P = \begin{pmatrix} R & S+\delta \\ R & S-\delta \end{pmatrix}$. Thus, $\binom{X}{Y} = Q\binom{U}{V}$ where $Q = P^{-1} = \frac{1}{2R\delta}\begin{pmatrix} \delta-S & \delta+S \\ R & -R \end{pmatrix}$. Then f is obtained from $\widehat{f}$ by the rule $f\binom{U}{V} = \widehat{f}\big(X\binom{U}{V}, Y\binom{U}{V}\big)$, that is, $f = \widehat{f}\circ Q$. Hence, in L,

$$a \;=\; f\binom{1}{0} \;=\; \widehat{f}\big(Q\binom{1}{0}\big) \;=\; \widehat{f}\binom{(\delta-S)/2R\delta}{1/2\delta} \quad\text{and}\quad b \;=\; f\binom{0}{1} \;=\; \widehat{f}\binom{(\delta+S)/2R\delta}{-1/2\delta}. \tag{7.5}$$

We have $A_{f,L} = L\{x,y\}$ where $f\binom{p}{q} = (px+qy)^3 = \big((x\ y)\binom{p}{q}\big)^3$ for all $p,q \in L^*$. Let $A_{\widehat{f},k} = k\{\widehat{x},\widehat{y}\}$, where $\widehat{f}\binom{p'}{q'} = \big((\widehat{x}\ \widehat{y})\binom{p'}{q'}\big)^3$ for all $p',q' \in k$. For any $p',q' \in k$, let $\binom{p}{q} = P\binom{p'}{q'}$, so $\binom{p'}{q'} = Q\binom{p}{q}$. Then, we have

$$\widehat{f}\binom{p'}{q'} \;=\; \widehat{f}\big(Q\binom{p}{q}\big) \;=\; f\binom{p}{q} \;=\; \big((x\ y)\binom{p}{q}\big)^3 \;=\; \big((x\ y)P\binom{p'}{q'}\big)^3.$$

If we set $(\widetilde{x}\ \widetilde{y}) = (x\ y)P$, then $\widehat{f}\binom{p'}{q'} = (\widetilde{x}\ \widetilde{y})\binom{p'}{q'}$ for all $p',q' \in k$. From this, we see that we can view $A_{\widehat{f},k}$ as a subalgebra of $A_{f,L}$ by setting $(\widehat{x}\ \widehat{y}) = (\widetilde{x}\ \widetilde{y}) = (x\ y)P$. Thus, $(x\ y) = (\widehat{x}\ \widehat{y})Q$; that is,

$$x \;=\; \tfrac{\delta-S}{2R\delta}\,\widehat{x} + \tfrac{1}{2\delta}\,\widehat{y} \quad\text{and}\quad y \;=\; \tfrac{\delta+S}{2R\delta}\,\widehat{x} - \tfrac{1}{2\delta}\,\widehat{y}. \tag{7.6}$$

Then $A_{\widehat{f},L} = L\{\widehat{x},\widehat{y}\} = A_{f,L}$. Let τ be the k-automorphism of L with $\tau(\delta) = -\delta$. We extend τ to an automorphism of $A_{\widehat{f},L} = A_{f,L}$ by setting $\tau(\widehat{x}) = \widehat{x}$ and $\tau(\widehat{y}) = \widehat{y}$, and extend τ further to $Q_{f,L} = q(A_{f,L})$. Thus, $A_{\widehat{f},k} = {A_{f,L}}^\tau$ and $Q_{\widehat{f},k} = {Q_{f,L}}^\tau$.

Now, put $\widehat{c} = -27\Delta_{\widehat{f}}$ and $\widehat{d} = -27\widehat{c}$, and let $\widehat{\mathcal{E}}$ and $\widehat{\mathcal{E}}'$ be the projective elliptic curves $\widehat{\mathcal{E}}\colon Y^2 = X^3 + \widehat{c}$ and $\widehat{\mathcal{E}}'\colon Y^2 = X^3 + \widehat{d}$. Let

$$\widehat{\mathcal{T}} \;=\; \big\{(0,\sqrt{\widehat{c}}),(0,-\sqrt{\widehat{c}}),\mathcal{O}\big\} \subseteq \widehat{\mathcal{E}}(k_s) \quad\text{and}\quad \widehat{\mathcal{T}}' \;=\; \big\{(0,\sqrt{\widehat{d}}),(0,-\sqrt{\widehat{d}}),\mathcal{O}\big\} \subseteq \widehat{\mathcal{E}}'(k_s).$$

Recall from §6 that $\Delta_{\widehat{f}} = \epsilon^6\Delta_f$, where $\epsilon = det(Q) = -1/(2R\delta) \in L^*$; so, $\tau(\epsilon) = -\epsilon$. Finally, in $A_{f,F}$, set

$$z' \;=\; \epsilon z,\quad \overline{z}' \;=\; \epsilon\overline{z},\quad \widehat{\mathfrak{r}} \;=\; z'\overline{z}' \;=\; \epsilon^2\mathfrak{r},\quad\text{and}\quad \widehat{\mathfrak{s}} \;=\; {z'}^3 + \sqrt{\widehat{c}} \;=\; \epsilon^3\mathfrak{s}.$$

Proposition 7.4. *With notation as above, for $\widehat{f}$ as in (7.4) we have the following:*

(a) $Z(A_{\widehat{f},k}) = k[\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}]$ *and* $\widehat{\mathfrak{s}}^2 = \widehat{\mathfrak{r}}^3 + \widehat{c}$. *Also,* $k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}) \cong k(\widehat{\mathcal{E}})$.

(b) *Let* $\widehat{K} = k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}})(\widehat{u})$, *where* $\widehat{u} = \omega z' + \omega^2\overline{z}'$, *which has minimal polynomial* $X^3 - \widehat{\mathfrak{r}}X - 2\widehat{\mathfrak{s}}$ *over* $k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}})$. *Then* $\widehat{K}$ *is a maximal subfield of* $Q_{f,k}$ *and* $\widehat{K} \cong k(\widehat{\mathcal{E}}')$.

(c) $Q_{\widehat{f},k}$ *is the cup product of the class of* b/a *in* $H^1(k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}),\widehat{\mathcal{T}})$ *with the class of* $\widehat{K}$ *in* $H^1(k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}),\widehat{\mathcal{T}}')$.

Proof. (a) (This was proved in [H_1, Th. 1.1′]. We give a more detailed argument here, since we need it for the rest of the proof.) Let $F = L(\omega)$ where $\omega^3 = 1$, $\omega \neq 1$. For convenience, we assume that $F \neq L$. (When $F = L$, the Proposition still holds, and the arguments are a subset of what is given here.) We use the same notation as from Proposition 7.2 and 7.3 for things associated to $Q_{f,F}$, i.e., $z, \overline{z}, \mathfrak{r}, \mathfrak{s}, \sigma, \rho, K$. Extend τ from L to F by setting $\tau(\omega) = \omega$, and extend τ likewise from $A_{f,L}$ (resp. $Q_{f,L}$) to $A_{f,F}$ (resp. $Q_{f,F}$). Since $\tau(\sigma) = -\sigma$, formulas (7.5) and (7.6) show that $\tau(a) = b$, $\tau(b) = a$, $\tau(x) = y$, and $\tau(y) = x$ in $A_{f,L}$. Furthermore, since $c = -27\Delta_f = -27\epsilon^6\Delta_{\widehat{f}}$, we have $\tau(\sqrt{c}) = -\sqrt{c}$. Also, $\tau(z) = \tau(yx - \omega yx) = -\omega\overline{z}$ and $\tau(\overline{z}) = -\omega^2 z$, so $\tau(\mathfrak{r}) = \mathfrak{r}$, while $\tau(\mathfrak{s}) = -\mathfrak{s}$. Hence, as $\tau(\epsilon) = -\epsilon$, we have $\tau(z') = \omega\overline{z}'z$, $\tau(\overline{z}') = \omega^2 z'$, $\tau(\widehat{\mathfrak{r}}) = \widehat{\mathfrak{r}}$, and $\tau(\widehat{\mathfrak{s}}) = \widehat{\mathfrak{s}}$. Since $Z(A_{f,L}) = L[\mathfrak{r},\mathfrak{s}] = L[\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}]$, we have $Z(A_{\widehat{f},k}) = Z(A_{f,L})^\tau = k[\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}]$. Also, $\widehat{\mathfrak{s}}^2 - \widehat{\mathfrak{r}}^3 = \epsilon^6(\mathfrak{s}^2 - \mathfrak{r}^3) = \epsilon^6 c = \widehat{c}$. Furthermore, since $L(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}) = L(\mathfrak{r},\mathfrak{s})$ is not algebraic over k but $L(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}})$ is algebraic over $k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}})$, it follows that $\widehat{\mathfrak{r}}$ must be transcendental over k, which implies that $k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}) \cong k(\widehat{\mathcal{E}})$.

(b) Let $\widetilde{k} = k(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}})$, $\widetilde{L} = L(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}) = L(\mathfrak{r},\mathfrak{s}) = \widetilde{k}\big(\sqrt{\Delta_{\widehat{f}}}\big)$, and $\widetilde{F} = F(\widehat{\mathfrak{r}},\widehat{\mathfrak{s}}) = F(\mathfrak{r},\mathfrak{s}) = \widetilde{L}(\omega)$. Recall that K is the field $\widetilde{F}(z)$, which is cyclic Galois over $\widetilde{F}$, and $K^\sigma = \widetilde{L}(u)$ where $u = z + \overline{z}$, and K^σ is cyclic Galois over $\widetilde{L}$. So, $K^\sigma = \widetilde{L}(z' + \overline{z}')$. The $\widetilde{F}$-automorphism ρ of K with $\rho(z) = \omega z$, $\rho(\overline{z}) = \omega^2\overline{z}$ also satisfies $\rho(z') = \omega z'$ and $\rho(\overline{z}') = \omega^2\overline{z}'$, since $\rho(\epsilon) = \epsilon$. Of the three conjugates $z' + \overline{z}'$, $\omega z' + \omega^2\overline{z}'$, $\omega^2 z' + \omega\overline{z}'$ over $\widetilde{L}$, τ fixes $\widehat{u} = \omega z' + \omega^2\overline{z}'$, while transposing the other two. Since $K^\sigma = \widetilde{L}(u) = \widetilde{L}(\widehat{u})$, it follows that for $K^{\sigma,\tau}$ $\big($meaning $(K^\sigma)^\tau\big)$ we have $K^{\sigma,\tau} = \widetilde{L}(\widehat{u})^\tau = \widetilde{k}(\widehat{u}) = \widehat{K}$. Hence, $\widehat{K}$ is a maximal subfield of $Q_{\widehat{f},k} = (Q_{f,F})^{\sigma,\tau}$. Set $\widehat{\mathfrak{r}}' = 6\sqrt{c}/(\omega z' - \omega^2\overline{z}')$ and $\widehat{\mathfrak{s}}' = 9\sqrt{c}(\omega z' + \omega^2\overline{z}')/(\omega z' - \omega^2\overline{z}')$ in K. Since $\tau(\sqrt{c}) = \sigma(\sqrt{c}) = -\sqrt{c}$ and $\tau(\omega z') = \sigma(\omega z') = \omega^2\overline{z}'$, we have $\widehat{\mathfrak{r}}', \widehat{\mathfrak{s}}' \in K^{\sigma,\tau} = \widehat{K}$. Because $(\omega z')^3 = \widehat{\mathfrak{s}} + \sqrt{\widehat{c}}$ and $(\omega z')(\omega^2\overline{z}') = \widehat{\mathfrak{r}}$ with $\widehat{\mathfrak{s}}^2 = \widehat{\mathfrak{r}}^3 + \widehat{c}$, the argument for Proposition 7.3 shows that $\widehat{\mathfrak{s}}'^2 = \widehat{\mathfrak{r}}'^3 + \widehat{d}$ and $\widehat{K} = k(\widehat{\mathfrak{s}}',\widehat{\mathfrak{r}}') \cong k(\mathcal{E}')$. Also, as $(\omega z')(\omega^2\overline{z}') = \widehat{\mathfrak{r}}$ and $(\omega z')^3 + (\omega\overline{z}')^3 = z'^3 + \overline{z}'^3 = 2\,\widehat{\mathfrak{s}}$, we have $\widehat{u}^3 = (\omega z' + \omega^2\overline{z}')^3 = \widehat{\mathfrak{r}}\,\widehat{u} + 2\,\widehat{\mathfrak{s}}$, which yields the minimal polynomial of $\widehat{u}$ over $\widetilde{k}$.

(c) We have $L\widehat{K} = K^\sigma$, which we have seen is cyclic Galois over $\widetilde{L}$ with $\mathcal{G}al(K^\sigma/L) = \langle \rho|_{K^\sigma}\rangle$ where ρ is the $\widetilde{F}$-automorphism of K with $\rho(z) = \omega z$ and $\rho(\overline{z}) = \omega^2\overline{z}$. Note that $\rho\tau(z) = \rho(-\omega\overline{z}) = -\overline{z} = \tau\rho^2(z)$, so $\rho\tau = \tau\rho^2$. So for the character $\chi \in H^1(\widetilde{L},\mathbb{Z}_3) = Hom(G_{\widetilde{L}},\mathbb{Z}_3)$ with kernel G_{K^σ} and mapping ρ to 1 $(mod\, 3)$, we have $\big(\tau(\chi)\big)(\rho) = \chi(\tau^{-1}\rho\tau) = \chi(\rho^{-1}) = -\chi(\rho)$; thus, $\tau(\chi) = \chi^{-1}$. This implies by Proposition 1.1 that χ is the image of some $\varphi \in H^1(\widetilde{k},\widehat{\mathcal{T}}')$ under the injective composition $H^1(\widetilde{k},\widehat{\mathcal{T}}') \cong H^1(\widetilde{k},\mathbb{Z}_3(\Delta_{\widehat{f}})) \xrightarrow{res} H^1(\widetilde{L},\mathbb{Z}_3)$. Similarly, since $\tau(b/a) = (b/a)^{-1}$, the image of b/a in $\widetilde{L}^*/\widetilde{L}^{*3}$ is the image of some $\psi \in H^1(\widetilde{k},\widehat{\mathcal{T}})$ under the injective map $H^1(\widetilde{k},\widehat{\mathcal{T}}') \cong H^1(\widetilde{k},\mu_3(\Delta_{\widehat{f}})) \xrightarrow{res} H^1(\widetilde{L},\mu_3) \cong \widetilde{L}^*/\widetilde{L}^{*3}$. Now, the map $Br(\widetilde{k}) \to Br(\widetilde{L})$ is injective on 3-torsion subgroups as $[\widetilde{L}\!:\!\widetilde{k}] = 2$. In order to see that $Q_{\widehat{f},k}$ is the cup product of φ with ψ, it suffices to check that $Q_{\widehat{f},L}$ is the cup product of $res_{\widetilde{k}\to\widetilde{L}}(\varphi)$ with $res_{\widetilde{k}\to\widetilde{L}}(\psi)$. But, this is clear from the isomorphism $Q_{\widehat{f},L} = Q_{f,L} \cong (K^\sigma/L,\rho,b/a)$ of Proposition 7.2, as $res_{\widetilde{k}\to\widetilde{L}}(\varphi)$ is χ,

whose kernel has fixed field K^σ, and $res_{\widetilde{k}\to\widetilde{L}}(\psi) = b/a \ (mod\ L^{*3})$. $\square$

We close with a remark on how $Q_{f,k}$ sits in $Br(\mathcal{E})$. To simplify notation, let $f(X,Y)$ be an arbitrary nondegenerate binary cubic form over a field k, and let $\mathcal{E}$ be the Jacobian of the projective curve $\mathcal{C}_f\colon Z^3 = f(X,Y)$. As we have seen, the ring of quotients $Q = Q_{f,k}$ of the Clifford algebra $A_{f,k}$ has center which can be identified with the function field of the projective elliptic curve $\mathcal{E}$. But more is known: Q is unramified at all the finite points of $\mathcal{E}$ because $A_{f,k}$ is an Azumaya algebra over the coordinate ring of the corresponding affine piece of $\mathcal{E}$; moreover, Q is also unramified at the infinite point $\mathcal{O}$ of $\mathcal{E}$, and its specialization at $\mathcal{O}$ is split, as shown in [H_1, p. 1275]. Therefore, $[Q]$ lies in $Br(\mathcal{E})$ the Brauer group of the elliptic curve $\mathcal{E}$. This $Br(\mathcal{E})$ has equivalent characterizations as: (1) the subgroup of $Br(k(\mathcal{E}))$ consisting of the classes of algebras unramified at all points of $\mathcal{E}$ (not just rational points); (2) the group of equivalence classes of sheaves of Azumaya algebras over the curve $\mathcal{E}$; (3) $H^2_{\text{ét}}(\mathcal{E},\mathbb{G}_m)$. There is a more explicit description of $Br(\mathcal{E})$, as $\mathcal{E}$ is a projective elliptic curve: Let $WC(\mathcal{E}) = H^1(k,\mathcal{E})$, the Weil-Châtelet group of $\mathcal{E}$, which classifies isomorphism classes of principal homogeneous spaces of $\mathcal{E}$ (cf. [Si, pp. 290-291]). There is a canonical short exact sequence

$$0 \longrightarrow Br(k) \longrightarrow Br(\mathcal{E}) \longrightarrow WC(\mathcal{E}) \longrightarrow 0,$$

which is split by the specialization map at the rational point $\mathcal{O}$ which sends $Br(\mathcal{E})$ to $Br(k)$. (See [Sk, p. 64] or [CK, (9)]. This is also deducible from the results in [L_2, §2].) Thus, we have

$$Br(\mathcal{E}) \ \cong\ Br(k) \oplus WC(\mathcal{E}). \tag{7.7}$$

Now, the curve $\mathcal{C}_f$ is a principal homogeneous space of $\mathcal{E}$, so it corresponds to some $\gamma_f \in WC(\mathcal{E})$. The class $[Q]$ in $Br(\mathcal{E})$ maps to γ_f in $WC(\mathcal{E})$, as was shown in [H_3, p. 518] though it was not stated that way. Thus, $[Q]$ in $Br(\mathcal{E})$ corresponds to $(0,\gamma)$ in $Br(k)\oplus WC(\mathcal{E})$. This illuminates the main result of [H_3], which says that B is split if and only if $\mathcal{C}_f$ has a rational point. For, C_f has a rational point if and only if $C_f \cong \mathcal{E}$ over k if and only if $\gamma_f = 0$ in $WC(\mathcal{E})$ if and only if $[Q] = 0$ in $Br(\mathcal{E})$ by (7.7).

REFERENCES

[A] A. A. Albert, On normal Kummer fields over a non-modular field, *Trans. Amer. Math. Soc.*, **36** (1934), 885-892.

[An] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis, Jacobians of genus one curves, *J. Number Theory*, **90** (2001), 304-315.

[Ca] J. W. S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, Cambridge, 1991.

[CK] M. Ciperiani and D. Krashen, Relative Brauer groups of genus 1 curves, preprint, arXiv:math/0701614v2.

[D] L. E. Dickson, *Algebraic Invariants*, J. Wiley, New York, 1914.

[Gr] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics, **776**, Springer, Berlin, 1980

[H_1] D. Haile, On the Clifford algebra of a binary cubic form, *Amer. J. Math.*, **106** (1984), 1269-1280.

[H_2] D. Haile, On Clifford algebras, conjugate splittings, and function fields of curves, in *Israel Math. Conf. Proc*, volume 1: Ring Theory 1989, in honor of S.A. Amitsur (L. Rowen, ed.) Weizman Science Press, Jerusalem, 356-361.

[H_3] D. Haile, When is the Clifford algebra of a binary cubic form split?, *J. Algebra*, **146** (1992), 514-520.

[HKRT] D. Haile, M.-A. Knus, M. Rost, and J.-P. Tignol, Algebras of odd degree with involution, trace forms and dihedral extensions, *Israel J. Math.*, **96** (1996), 299-340.

[Hu] D. Husemöller, *Elliptic Curves*, 2nd ed., Springer, New York, 1987.

[J] N. Jacobson, *Finite Dimensional Division Algebras over Fields*, Springer, Berlin, 1996.

[KMRT] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol, *The Book of Involutions*, Amer. Math. Soc., Providence, RI, 1998.

[L_1] S. Lichtenbaum, The period-index problem for elliptic curves, *Amer. J. Math.*, **90** (1968), 1209-1223.

[L_2] S. Lichtenbaum, Duality theorems for curves over p-adic fields, *Invent. Math.*, **7** (1969), 120-136.

[Mi] J. S. Milne, *Class Field Theory*, http://www.jmilne.org/math/CourseNotes/CFT400.pdf

[SAGE] *SAGE Mathematical Software*, Version 2.6, http://www.sagemath.org.

[Se] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[Sk] A. Skorobogatov, *Torsors and Rational Points*, Cambridge University Press, Cambridge, 2001.

[V] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris, Sér. A-B*, **273** (1971), A238-A241.

Department of Mathematics
Indiana University
Bloomington, IN 47405

e-mail: haile@indiana.edu

Department of Mathematics
California State University
San Bernardino, CA 92407

e-mail: ihan@csusb.edu

Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112

e-mail: arwadsworth@ucsd.edu